Lietuvos nacionalinė Martyno Mažvydo biblioteka
Informacijos politikos ir analitikos departamentas
Informacijos analitikos skyrius

Biuletenio tematika ir tema
Tarptautiniai santykiai ir geopolitika

Biuletenio laidos antraštė, probleminis klausimas
Povandeninės infrastruktūros apsauga: techniniai ir politiniai aspektai

Esminiai žodžiai
Kinija, Jungtinės Amerikos Valstijos, Rusija, povandeninė infrastruktūra, ryšiai, energetika, vamzdynai, kabeliai, povandeninės infrastruktūros apsauga, diversijos, kibernetinis saugumas

Serija ir registracijos numeris
ZD-2025-3

Leidimo data
2025-03-07

Leidimo vieta
Vilnius

Žanras
☒ Analitinė apžvalga ☐ Kita

Šaltiniai: kategorijos
☐ Teisės aktai ☐ Politinė komunikacija
☒ Analitinių centrų kūriniai / leidiniai
☒ Žiniasklaidos turinys ☐ Socialinių tinklų turinys
☐ Statistiniai duomenys ☐ Mokslo darbai
☐ Metainformaciniai produktai
☐ Išviešinti slapti / privatūs duomenys

Šaltiniai: nuo – iki
2019 07 03 – 2025 03 04

Šaltiniai: kalbos
☒ Lietuvių k. ☐ Lenkų k.
☒ Anglų k. ☐ Kitos ES kalbos
☐ Rusų k. ☐ Kitos

Citavimui (APA stiliumi)
Nacionalinė biblioteka, Informacijos analitikos skyrius (2025). *Povandeninės infrastruktūros apsauga: techniniai ir politiniai aspektai* (ZD-2025-3). Vilnius.

Kontaktiniai duomenys
Informacijos analitikos skyrius; analitika@lnb.lt. Nacionalinė biblioteka, Gedimino pr. 51, 01109 Vilnius.

Turinio apžvalga
Šiame analitiniame darbe aptariama:
- povandeninė infrastruktūra: vamzdynai, ryšio kabeliai, energetinės jungtys;
- povandeninės kritinės infrastruktūros gadinimo problema;
- pasaulinis ryšio kabelių tinklas;
- Kinijos technologinės plėtros keliami pavojai.

1. Įžanga

Povandeninę kritinę infrastruktūrą galima suskirstyti į tris stambias kategorijas:

- vamzdynus,
- elektros jungtis,
- ryšio kabelius.

Šioje apžvalgoje nagrinėjami tokios infrastruktūros apsaugos klausimai.

Tiek po vandeniu nutiesti vamzdžiai, tiek kabeliai gali būti pažeisti netyčia ar vykdant diversijas, tačiau vamzdynai kelia didesnę ekologinę grėsmę nei kabeliai, ypač turint omenyje tai, kad pirmieji

povandeniniai naftos gręžiniai atsirado maždaug prieš 80 metų. Skaičiuojama, kad šiuo metu po vandeniu paklota apie 20 tūkst. km vamzdžių, daugiausia skirtų naftos, jos produktų ir gamtinių dujų eksportui.[1] Laiku neatnaujinta infrastruktūra tampa pavojinga aplinkai.[2] Pažeistų vamzdynų remontas yra techniškai sudėtingesnė ir brangesnė užduotis nei kabelių taisymas.

Apžvalgoje daugiausia susitelkta į ryšio kabelių saugumo techninius ir politinius aspektus, nes šie kabeliai sudaro pasaulinio interneto karkasą, jais perduodama 99 proc. tarpžemyninių elektroninių signalų. Dirbtinių žemės palydovų vaidmuo perduodant informaciją nėra toks reikšmingas.

Kabelių pažeidimai gali kritiškai paveikti duomenų perdavimą, tarptautines finansines operacijas ir kitus svarbius komunikacijos procesus – kitaip tariant, visiškai sutrikdyti daugelio šalių ūkio funkcionavimą. Povandeninių ryšių kabelių saugos akcentas yra ne vien fizinė apsauga, bet ir **šnipinėjimo bei kibernetinių diversijų prevencija**. Šioms problemoms nemažai dėmesio skiria Lietuvos žinybos, juolab kad pastaruoju metu šaliai svarbi infrastruktūra tapo diversijų objektu.

Apžvalgoje nušviečiamas ir apsaugos problemų politinis fonas, būtent Jungtinių Amerikos Valstijų (JAV) ir jų sąjungininkų **geopolitinė konkurencija su Kinija**, pasireiškianti infrastruktūros plėtros srityje. Pvz., JAV bandymas išstumti Kiniją iš povandeninių kabelių tiesimo ir eksploatavimo rinkos jau vadinamas **„šaltuoju karu po vandeniu"**,[3] o politiniu, kultūriniu ir juridiniu aspektais galima įžvelgti spartėjantį pasaulio pasidalijimą į laisvo ir nelaisvo interneto sritis.[4]

2. Diversijos prieš povandeninę infrastruktūrą Baltijos jūroje

Lietuvos viešojoje erdvėje pastaruoju metu dažnai aptariama mūsų šalies kaimynystėje esantiems vamzdynams ir elektros jungtims daroma žala. Ryškiausi tokio pobūdžio incidentai:

- dujotiekio „Nord Stream" sprogimai Baltijos jūroje 2022 metų rudenį,[5]
- elektros kabelių gadinimas Baltijos jūroje (nuo 2023 metų spalio pažeista mažiausiai 11 Baltijos jūros dugnu nutiestų kabelių).[6]

„Nord Stream" atvejis – išskirtinė diversija, kurios kaltininkų vis dar ieškoma. Mokslininkų skaičiavimais, per dujotiekio sprogimus į aplinką pateko apie 465 tūkst. tonų šiltnamio efektą sukeliančių metano dujų –

[1] Walsh, D. (2023 m. kovo mėn.). Seafloor Cables and Pipelines: Are They Secure? Prieiga per internetą: *https://www.usni.org/magazines/proceedings/2023/march/seafloor-cables-and-pipelines-are-they-secure*
[2] A Timeline of Subsea Innovation in the Oil & Gas Industry 1940-2000. (2021 m. liepos 19 d.). Prieiga per internetą: *https://www.viperinnovations.com/a-timeline-of-subsea-innovation-in-the-oil-gas-industry-1940-2000-part-one/*
[3] Be ready for the new Cold War, under the sea. (2025 m. sausio 10 d.). Prieiga per internetą: *https://www.japantimes.co.jp/editorials/2025/01/10/cold-war-under-the-sea/*
[4] Zandt, F. (2021 m. rugsėjo 22 d.). Is Free Internet a Myth? Prieiga per internetą: *https://www.statista.com/chart/3942/internet-freedom-across-the-world-visualized/*
[5] Ambrose, T., Belam, M., Sullivan, H. (2022 lapkričio 18 d.). Russia-Ukraine war: remains of explosives found at Nord Stream pipeline blast site – as it happened. Prieiga per internetą: *https://www.theguardian.com/world/live/2022/nov/18/russia-ukraine-war-live-missile-strikes-leave-10-million-ukrainians-without-power-says-zelenskiy*
[6] Per 15 mėnesių nukentėjo mažiausiai 11 kabelių: kas vyksta Baltijos jūroje? (2025 m. sausio 28 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/2471905/per-15-menesiu-nukentejo-maziausiai-11-kabeliu-kas-vyksta-baltijos-juroje*

Analitinių apžvalgų archyvas: *https://lnb.lt/istekliai/kiti-istekliai/analitines-apzvalgos*

tai didžiausias metano kiekis, į atmosferą patekęs per vieną žmogaus sukeltą įvykį.[7] Nors „Nord Stream" šiuo metu nefunkcionuoja, esama lūkesčių, kad dalis vamzdyno, jį suremontavus, gali būti panaudota vandenilio transportavimui iš Suomijos į Vokietiją.[8]

Baltijos jūroje nutiestų kabelių gadinimas, esant įtarimų, kad tai **Rusijos diversija**, sukėlė nukentėjusiųjų valstybių, taip pat ir Lietuvos, atsaką. Sustiprintas Danijos, Švedijos, Lietuvos, Latvijos, Estijos ir kitų NATO valstybių patruliavimas Baltijos jūroje.[9] Lietuvai kritiškai svarbūs šie objektai, kuriems galima pakenkti jūroje:

- suskystintųjų gamtinių dujų laivas-saugykla,
- Būtingės naftos terminalas,
- elektros jungtis su Švedija Baltijos jūros dugnu (aptikta būtent šios jungties pažeidimo pėdsakų; incidentas galimai vyko 2024 metų rudenį[10]).

Įtariama, kad ryšio ir elektros kabeliai 2024 metų rudenį ir žiemą taip pat tapo tyčinių veiksmų takiniais. Lietuvai reikšmingų 2024 m. incidentų sąrašas:[11, 12]

- nutrauktas Lietuvą ir Švediją jungiantis 218 km ilgio ryšio kabelis „BCS East-West" (tąkart buvo pažeistas ir 1 172 km ilgio kabelis „C-Lion1", jungiantis Suomiją ir Vokietiją), apie incidentą pranešta 2024 m. lapkričio 19 d.
- Nekritiškai apgadinta elektros jungtis „Nordbalt" tarp Lietuvos ir Švedijos – 450 km ilgio nuolatinės srovės aukštos įtampos kabelis. Apie incidento, kurio laikas nežinomas, požymius pranešta 2025 m. sausio 13 d.

Atsižvelgdami į povandeninių komunikacijų ilgį ir turimas apsaugos galimybes NATO pareigūnai teigia, kad fiziškai **neįmanoma apsaugoti kiekvieno infrastruktūros metro**, tačiau būtina stebėti įtartinus laivus, galimai vykdančius diversines ir žvalgybines užduotis.[13]

Verta pažymėti, kad **Rusija daug mažiau priklausoma nuo povandeninių kabelių nei JAV ar Kinija**, nes yra žemyninė valstybė. Ji mažiau pažeidžiama dėl povandeninės infrastruktūros sutrikimų, galbūt

[7] Mokslininkų teigimu, per „Nord Stream" sprogimus į aplinką pateko 465 000 tonų metano. (2025 m. sausio 16 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/mokslas-ir-it/11/2462149/mokslininku-teigimu-per-nord-stream-sprogimus-i-aplinka-pateko-465-000-tonu-metano*
[8] Wettengel, J. (2025 m. vasario 5 d.). German government and industry consider return of Nord Stream pipeline – media report. Prieiga per internetą: *https://www.cleanenergywire.org/news/german-government-and-industry-consider-return-nord-stream-pipeline-media-report*
[9] Gaižauskaitė, J. (2025 m. vasario 21 d.). Baltijos jūroje – vis daugiau incidentų, tačiau Lietuva teturi 40 metų senumo karo laivų. Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/2494329/baltijos-juroje-vis-daugiau-incidentu-taciau-lietuva-teturi-40-metu-senumo-karo-laivu*
[10] Deveikis, J. (2025 m. sausio 16 d.). Nepavykęs bandymas: ką Lietuvai reikštų nutrauktas elektros kabelis su Švedija? Prieiga per internetą: *https://www.lrt.lt/naujienos/verslas/4/2459188/nepavykes-bandymas-ka-lietuvai-reikstu-nutrauktas-elektros-kabelis-su-svedija*
[11] Savickas, E. (2024 m. lapkričio 19 d.). Vienas nutrauktas, liko dar du: kaip apsergėti šimtus kilometrų Lietuvą jungiančių kabelių. Prieiga per internetą: *https://www.lrt.lt/naujienos/verslas/4/2417945/vienas-nutrauktas-liko-dar-du-kaip-apsergeti-simtus-kilometru-lietuva-jungianciu-kabeliu*
[12] Švedija ant „Nordbalt" kabelio Baltijos jūroje aptiko apgadinimo ženklų. (2025 m. sausio mėn. 13 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/2459049/svedija-ant-nordbalt-kabelio-baltijos-juroje-aptiko-apgadinimo-zenklu*
[13] NATO vadovas: neįmanoma apsaugoti visos povandeninės infrastruktūros. (2025 m. sausio 16 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/2462327/nato-vadovas-neimanoma-apsaugoti-visos-povandenines-infrastrukturos*

Analitinių apžvalgų archyvas: *https://lnb.lt/istekliai/kiti-istekliai/analitines-apzvalgos*

todėl yra labiau linkusi išnaudoti kitų šalių pažeidžiamumą šioje srityje.[14] Lietuvai svarbios infrastruktūros apsauga neatsiejama nuo Baltijos baseino valstybių ir, plačiau žvelgiant, NATO pastangų.

3. Pasaulinis povandeninių kabelių tinklas

Povandeninių kabelių infrastruktūra apima ilgesnes ar trumpesnes šviesolaidinio ryšio linijas, energetines jungtis tarp didelių elektros tinklų ir lokalias ryšio bei elektros jungtis su vėjo jėgainėmis, naftos gavybos platformomis.

Šiuo metu esama **per 500 veikiančių ar planuojamų eksploatuoti povandeninių ryšio kabelių**, kurių galutinių ir tarpinių pakrantės pastočių skaičius siekia maždaug 1 400. Kabeliais, kurių **bendrasis ilgis pasaulyje siekia 1,4 mln. km, perduodama apie 99 proc. tarpžemyninių duomenų.**[15]

Visų rūšių povandeninių kabelių tiesimo ir eksploatavimo pasaulinės **rinkos vertė 2022 m. siekė 27,57 mlrd. JAV dolerių**,[16] prognozuojama, kad iki 2030 m. ji gali išaugti iki 30,5 mlrd. JAV dolerių.[17]

Kabeliai sudaro pasaulinių telekomunikacijų bei interneto pagrindą. Jie yra daug pralaidesni, efektyvesni, ekonomiškesni ir **patikimesni nei kosminiai ryšio palydovai**. Vartotojų duomenys (pvz., elektroninio pašto serveriai, „debesų" įranga ir programų duomenys) dažnai saugomi įvairiose pasaulio vietose įsikūrusiuose duomenų centruose. Ši infrastruktūra veiksmingai palengvina tiek kasdienį naudojimąsi internetu, tiek finansines operacijas. Pavyzdžiui, pasaulinės prekybos valiuta operacijos, kurių neįmanoma atlikti be tarpžemyninio ryšio, 2022 metų balandį pasiekė **7,51 trln. JAV dolerių per dieną** apimtį.[18]

Pažeidžiami vyriausybiniai ryšiai taip pat labai priklauso nuo povandeninės infrastruktūros. Užšifruoti valstybinės reikšmės pranešimai perduodami komercinėmis interneto linijomis.[19]

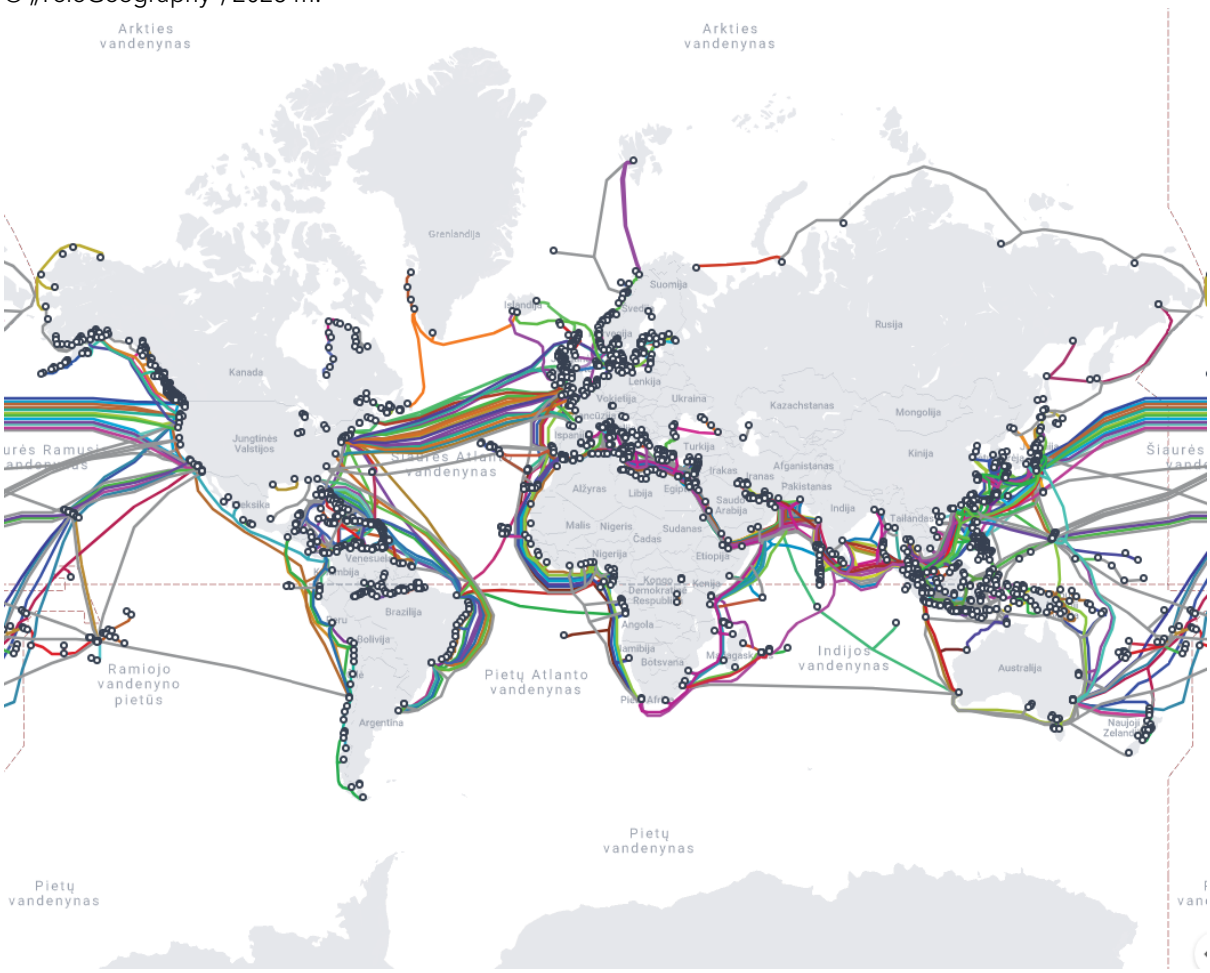
Numatoma, kad vykstant dirbtinio intelekto (DI) revoliucijai smarkiai išaugs duomenų apdorojimo ir skaitmeninės informacijos saugojimo pajėgumų paklausa. Didelių kalbos modelių duomenims tvarkyti ir laikyti reikės gigantiškos talpos saugyklų. Jeigu DI centrai, kaip rodo dabartinės tendencijos, išsidėstys įvairiose šalyse, jiems sujungti reikės papildomos povandeninės infrastruktūros.[20] Be to, dėl DI

[14] Runde, D., Murphy, E., Bryja T. (2024 m. rugpjūčio 16 d.). Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition. Prieiga per internetą: *https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition*
[15] Gross, A., Heal, A. Campbell, C. Clark, D., Bott, I., De la Torre Arenas, I. (2023 m. birželio 13 d.). How the US is pushing China out of the internet's plumbing. Prieiga per internetą: *https://ig.ft.com/subsea-cables/*
[16] Submarine Cables Market Size, Share & Trends Report 2023 - 2030. (n. d.). Prieiga per internetą: *https://www.grandviewresearch.com/industry-analysis/submarine-cables-market*
[17] Submarine Cable System Market Worth $30.50 Billion, Globally, by 2030. (2024 m. rugpjūčio 28 d.). Prieiga per internetą: *https://www.globenewswire.com/news-release/2024/08/28/2937018/0/en/Submarine-Cable-System-Market-Worth-30-50-Billion-Globally-by-2030-Exclusive-Report-by-The-Insight-Partners.html*
[18] Stefanova, Z. (2025 m. sausio 29 d.). Forex Daily Trading Volume. Prieiga per internetą: *https://www.bestbrokers.com/forex-trading/forex-daily-trading-volume/*
[19] Žr. 14 šaltinį.
[20] Ten pat.

technologijų diegimo **pašoks ir elektros energijos poreikis**. Antai Airijai ir Singapūrui teko pristabdyti DI duomenų centrų plėtrą, nes **elektros tinklų apkrovos pasiekė kritinę ribą**.[21]

Pasaulinės DI rinkos vertė 2024-iais buvo maždaug 306 mlrd. JAV dolerių. Prognozuojama, kad ši rinka iki 2030 m. kasmet augs apie 28,5 proc. Tyrimai rodo, kad bent 58 proc. kompanijų ketina kokia nors forma investuoti į DI. Apie 51 proc. kompanijų naudoja vadinamąjį *generatyvinį* DI (GDI) turinio kūrimui, veiklos automatizavimui ir vartotojų aptarnavimui, 31 proc. įmonių ketina įvairiais būdais kelti darbuotojų kvalifikaciją DI sferoje. GDI rinka 2032 m. gali siekti 1,3 trln. JAV dolerių.[22] Esant tokioms perspektyvoms, įvairaus pobūdžio duomenų apsauga tampa vis aktualesnė.

1 žemėlapis. Pasaulinis povandeninių ryšio kabelių tinklas.
© „TeleGeography“, 2025 m.[23]



Apibendrinant galima teigti, kad povandeniniai ryšio kabeliai sudaro globalizuotos, skaitmena paremtos pasaulinės ekonomikos informacinį karkasą, kuriam šiuo metu nėra (ir greitu laiku neatsiras) alternatyvos.

[21] Bennett, G. (2024 m. lapkričio 18 d.). The Impact of Artificial Intelligence on Submarine Networks. Prieiga per internetą: *https://www.marinetechnologynews.com/news/impact-artificial-intelligence-submarine-642397*
[22] AI statistics and trends: New research for 2025. (2025 m. vasario 7 d.). Prieiga per internetą: *https://www.hostinger.com/tutorials/ai-statistics?utm_medium=ppc&utm_campaign=Generic-Tutorials-DSA|NT:Se|LO:LT-t2&gad_source=1&gclid=CjwKCAiAlPu9BhAjEiwA5NDSA0NPlbIjWwfMUxPlIVapgnEXnBlORabCnIGnTAMNUnLcQKjRTphzKxoCupoQAvD_BwE#Top_10_AI_stats_you_should_know_for_2025*
[23] TeleGeography. (2025 m. kovo 3 d.). Submarine Cable Map. Prieiga per internetą: *https://www.submarinecablemap.com/*

Analitinių apžvalgų archyvas: *https://lnb.lt/istekliai/kiti-istekliai/analitines-apzvalgos*

4. Kinijos infrastruktūros plėtros iniciatyvų keliami pavojai

Kabeliai dažniausiai priklauso daugiau nei vienam savininkui, vartotojai šios infrastruktūros pajėgumus nuomoja. Tiesiant ir aptarnaujant kabelius ilgą laiką **dominavo Prancūzijos, JAV ir Japonijos bendrovės**. Maždaug prieš dešimtmetį į pasaulinę kabelių rinką ėmė skverbtis Kinijos valstybinis kapitalas, **tačiau kelios viena kitą pakeitusios JAV administracijos sugebėjo pristabdyti kinų pastangas**. Amerikiečiai nerimavo dėl galimo šnipinėjimo ir dėl to, kad karinio konflikto atveju Pekinas gali trikdyti Kinijos valdomų strateginių objektų veiklą.[24]

2020 m. JAV Vyriausybė pradėjo abiejų Jungtinių Valstijų politinių partijų palaikomą iniciatyvą „Švarus tinklas" (angl. *Clean Network*), pagal kurią teisinėmis priemonėmis uždrausta tiesti naujus kabelius, tiesiogiai jungiančius JAV su Kinija ar Honkongu.[25] JAV valdžia užkirto kelią kompanijų „Meta" ir „Google" pradėtam kabelio, kuris turėjo sujungti Ameriką su Honkongu, projektui, todėl ši linija buvo nutiesta tik iki Filipinų ir Taivano.[26]

Nors Kinijos siekis tapti svarbia pasaulinės povandeninių kabelių rinkos veikėja dabar smarkiai ribojamas, **Pekinas randa būdų įveikti kliūtis**. Kinijos Vyriausybei priklausančios telekomunikacijų bendrovės bando nukreipti savo pastangas į regionus, kuriuose ši valstybė vis dar turi komercinės ir politinės įtakos: Aziją, Afriką ir Lotynų Ameriką.

Pvz., Azijoje, kur kabelinio ryšio paklausa auga greičiau nei daugelyje kitų pasaulio regionų, kompanijos „China Telecom", „China Mobile" ir „China Unicom" šiuo metu vykdo kelis stambius kabelių projektus, tarp kurių – linijų, sujungsiančių Kiniją su Singapūru ir Japonija, tiesimas.[27]

Kinijos politika tiesiant povandeninius kabelius glaudžiai susijusi su šalies įgyvendinama **iniciatyva „Viena juosta, vienas kelias" (angl. – Belt and Road Initiative)**. Pagal 2013 m. startavusią iniciatyvą numatytos milžiniškos Kinijos investicijos į įvairius infrastruktūros plėtros projektus skirtingose pasaulio vietose. Kinijos pateikiamais duomenimis, iniciatyvoje 2023 m. dalyvavo 150 šalių.[28]

Kinija „Vienos juostos, vieno kelio" iniciatyvą pradėjo kaip atvirą susitarimą, kuriame kviečiamos dalyvauti visos šalys. Pasaulio banko skaičiavimais, apie 70 valstybių, geografiškai išsidėsčiusių palei „Vienos juostos, vieno kelio" transporto koridorių, 2017 m. pritraukė maždaug 35 proc. visų tiesioginių užsienio investicijų ir sudarė apie 40 proc. pasaulinio eksporto. 2017 m. planuota į įvairius šių „transporto koridoriaus" šalių, tarp kurių – ir pati Kinija, infrastruktūros projektus investuoti 575 mlrd. JAV dolerių – daugiausiai Kinijos kapitalo. Skaičiuota, kad užbaigus iniciatyvos aprėptyje vystomus transporto projektus prekių gabenimas pagreitėtų 12 proc., prekybos apimtis galėtų augti iki maždaug 10 proc. Tai turėjo pagyvinti į projektus įtrauktų šalių ekonomikas ir leisti 7,6 mln. žmonių išbristi iš skurdo.[29] Tačiau, praėjus dešimtmečiui nuo projekto pradžios, juntamas tiesioginių užsienio investicijų į „Vienos juostos, vieno kelio" projektus sumažėjimas. Dėl lėto Kinijos ekonomikos atsigavimo po COVID-19 pandemijos, nekilnojamojo turto problemų, didėjančios vidaus skolos ir kitokių ekonominių sunkumų valstybės įmonės ne visuomet pajėgia palaikyti stambius infrastruktūros projektus, kurių kažkada ėmėsi pagal minėtą iniciatyvą. Todėl nuo 2021 m. Kinijos valstybinė administracija propaguoja naują „mažų ir gražių" (angl. *small and beautiful*) investicijų į

[24] Gross, A., Heal, A. Campbell, C. Clark, D., Bott, I., De la Torre Arenas, I. (2023 m. birželio 13 d.). How the US is pushing China out of the internet's plumbing. Prieiga per internetą: *https://ig.ft.com/subsea-cables/*
[25] Fidler, D. (2020 m. spalio 5 d.). The Clean Network Program: Digital Age Echoes of the "Long Telegram"? Prieiga per internetą: *https://www.cfr.org/blog/clean-network-program-digital-age-echoes-long-telegram*
[26] Žr. 24 šaltinį.
[27] Ten pat.
[28] Statista. (2024 m. spalio 17 d.). Number of countries that have joined China's Belt and Road Initiative (BRI) as of December 2023, by continent. Prieiga per internetą: *https://www.statista.com/statistics/1347393/china-number-of-bri-partner-countries-by-region/*
[29] Belt and Road Initiative. (2018 m. kovo 29 d.). Prieiga per internetą: *https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative*

„Vieną juostą, vieną kelią" modelį. Siekiama, kad nauji projektai būtų mažesni, ekologiškesni ir finansiškai ne tokie rizikingi.[30]

Nuo 2015 m. Kinijos vykdoma tarptautinė **„Skaitmeninio šilko kelio" iniciatyva**[31] yra „Vienos juostos, vieno kelio" dalis. „Skaitmeninis šilko kelias" apima Kinijos politinę ir ekonominę paramą bei kitokią pagalbą valstybėms gavėjoms. Pagal šią iniciatyvą teikiama parama Kinijos eksportuotojams, įskaitant daugelį pasaulyje žinomų Kinijos technologijų įmonių, tarp kurių – „Huawei". „Skaitmeninio šilko kelio" projektais siekiama gerinti šalių telekomunikacijų tinklus, DI galimybes, „debesų" kompiuteriją, elektroninę prekybą, mobiliojo mokėjimo sistemas, stebėjimo technologijas ir kitas sritis. Iniciatyvoje „Viena juosta, vienas kelias" dalyvaujančios vyriausybės ir įmonės gali naudotis lengvatinėmis mažų palūkanų Kinijos paskolomis kiniškoms technologijoms įsigyti.[32]

Įvairiais duomenimis, apie trečdalis „Vienos juostos, vieno kelio" iniciatyvoje dalyvaujančių šalių bendradarbiauja pagal „Skaitmeninio šilko kelio" projektus. Pavyzdžiui, Kinija skiria didesnį finansavimą Afrikos informacijos ir ryšių technologijoms nei visos tarptautinės agentūros ir išsivysčiusios demokratinės valstybės kartu sudėjus.[33] Apskritai prognozuojama, kad **iki 2040 m. pasaulio infrastruktūros finansavimo deficitas pasieks beveik 15 trln. JAV dolerių**[34]. Su „Viena juosta, vienu keliu" susijusios investicijos gali bent iš dalies užpildyti šią spragą.

COVID-19 pandemija, kurios metu daugelis vyriausybių ėmė atidžiau stebėti savo gyventojus, prisidėjo prie kiniškų telekomunikacijų ir stebėjimo priemonių paklausos augimo besivystančiose šalyse. Reaguodamas į tai, Pekinas susiejo „Skaitmeninį šilko kelią" su **„Sveikatos šilko keliu"**, – dar viena „Vienos juostos, vieno kelio" iniciatyvos atšaka, skirta sveikatos apsaugos infrastruktūros plėtrai.

Kinija per COVID-19 pandemiją ėmė siekti pasaulinės lyderystės sveikatos apsaugos srityje. Dažnai pagalba teikta tiesiogiai per Kinijos ambasadas, pvz., Malaizijoje, Filipinuose, Graikijoje. Medicinos reikmenys tiekti ir per „Vienos juostos, vieno kelio" projektus vykdančias Kinijos įmones. „Jack Ma" ir „Alibaba" fondai pristatė pagalbos paketus daugybei šalių, tarp kurių – Uganda, Ukraina, netgi JAV. Kinija taip pat suteikė ekonominę paramą daugybei nukentėjusių šalių, įskaitant Šri Lanką, gavusią iš kinų 500 mln. JAV dolerių lengvatinę paskolą. Be to, Kinija koordinavo daugiašalius forumus COVID-19 klausimais.[35]

Pekinas pastaruoju metu laiko „Skaitmeninį šilko kelią" svarbiu užsienio politikos prioritetu, nes vis daugiau išsivysčiusių šalių, įskaitant JAV, Australiją, Japoniją ir kai kurias Europos valstybes, uždraudė Kinijos technologijų įmonėms naudotis savo 5G infrastruktūra ir plėtoti platesnes strategijas.

[30] Yeung, C. (2024 m. kovo 19 d.). The Belt and Road Initiative 10 Years Later: China's Transition to 'Small and Beautiful'. Prieiga per internetą: *https://www.asiapacific.ca/publication/china-belt-and-road-initiative-10-years-later*
[31] Assessing China's Digital Silk Road Initiative. A Transformative Approach to Technology Financing or a Danger to Freedoms? (n. d.). Prieiga per internetą: *https://www.cfr.org/china-digital-silk-road/*
[32] Zou, R. (2020 m. spalio 29 d.). China's Digital Silk Road: A Pathway to Post-Pandemic Economic Recovery? Prieiga per internetą: *https://research.hktdc.com/en/article/NTY5NjM4MTY0*
[33] Žr. 31 šaltinį.
[34] Kaldany, R., Losavio, J. (2019 m. balandžio 11 d.). The world is facing a $15 trillion infrastructure gap by 2040. Here's how to bridge it. Prieiga per internetą: *https://www.weforum.org/stories/2019/04/infrastructure-gap-heres-how-to-solve-it/*
[35] Lancaster, K., Rubin, M., Rapp-Hooper, M. (2020 m. balandžio 10 d.). Mapping China's Health Silk Road. Prieiga per internetą: *https://www.cfr.org/blog/mapping-chinas-health-silk-road*

Kai kurios besivystančios šalys, pvz., Indija, dėl Kinijos technologijų skverbimosi išreiškė panašų nepasitenkinimą kaip JAV ir Europa. „Skaitmeninio šilko kelio“ projektuose dalyvaujančios Kinijai draugiškos šalys, pvz., Mianmaras ir Malaizija, irgi išreiškė susirūpinimą dėl didėjančios valstybinės skolos, kurios augimą skatina kiniški projektai, ir jų suverenitetui kylančio pavojaus.[36]

Pekinui vis ryžtingiau vystant veiklas pasauliniu mastu apskritai nuogąstaujama, kad Kinija, pasitelkusi „Skaitmeninį šilko kelią“, gali šalims gavėjoms įpirši kiniškomis technologijomis pagrįstą autoritarizmo modelį. Kinijos technologijų įmonės jau padėjo kitų šalių vyriausybėms kuriant ir diegiant stebėjimo sistemas, kurios gali būti panaudotos prieš opozicines jėgas. Taip pat rengti mokymai, kaip stebėti ir cenzūruoti interneto turinį realiuoju laiku (*on-line* režimu). Nors kai kurios tokios Kinijos įmonės yra formaliai privačios, pagal Kinijos kibernetinio saugumo įstatymus jos privalo saugoti duomenis Kinijos teritorijoje esančiuose serveriuose, taigi tie duomenys gali būti prieinami Kinijos valdžios institucijoms.[37] Leidus kinų įmonėms kurti kitų šalių penktosios kartos mobiliojo ryšio tinklus ir kitą infrastruktūrą bei nustatyti technologijų standartus, kurie taptų norma ne vienoje valstybėje, gali kilti pavojus, kad Kinija šnipinės ir darys spaudimą jų politikos elitui, pasitelks neteisėtai gautus duomenis ir panaudos juos šantažui.[38]

5. Povandeninės infrastruktūros pažeidžiamumo veiksniai

Povandeninių kabelių pažeidimų pasitaiko gana dažnai – kasmet nutraukiama nuo 100 iki 150 kabelių, daugiausia užkabinus žvejybos įranga ar inkarais. Vienas kabelio remontas gali atsieiti iki 3 mln. JAV dolerių.[39] **Dažniausiai kabeliai pažeidžiami netyčia**, paprastai dėl atsitiktinio žmonių poveikio.[40] Vis dėlto, povandeninė infrastruktūra yra ir lengvas taikinys diversantams.

2023 m. Taivano valdžia apkaltino du Kinijos laivus nutraukus vienintelius du povandeninius kabelius, tiekiančius internetą į Taivano Matsu salas. Dėl incidento 14 tūkst. salos gyventojų šešias savaites patyrė skaitmeninę izoliaciją. Taivano oficialūs asmenys teigia, kad Kinijos laivai dažnai kelia įtarimų dėl kabelių gadinimo (27 atvejai nuo 2018-ųjų metų).[41]

Fizinio kabelių gadinimo pavojus yra realus, tačiau mažai tikėtina, kad taikos sąlygomis tokio pobūdžio diversijos prieš kurią nors valstybę galėtų pasiekti kritinį mastą. Dabartinio „šaltojo karo po vandeniu“ pagrindinė grėsmė yra **kabeliais perduodamų duomenų šnipinėjimas pasitelkiant povandeninę infrastruktūrą**.

[36] Assessing China's Digital Silk Road Initiative. A Transformative Approach to Technology Financing or a Danger to Freedoms? (n. d.). Prieiga per internetą: *https://www.cfr.org/china-digital-silk-road/*
[37] Ten pat.
[38] Ten pat.
[39] Submarine Cable System Market Worth $30.50 Billion, Globally, by 2030. (2024 m. rugpjūčio 28 d.). Prieiga per internetą: *https://www.globenewswire.com/news-release/2024/08/28/2937018/0/en/Submarine-Cable-System-Market-Worth-30-50-Billion-Globally-by-2030-Exclusive-Report-by-The-Insight-Partners.html*
[40] Runde, D., Murphy, E., Bryja T. (2024 m. rugpjūčio 16 d.). Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition. Prieiga per internetą: *https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition*
[41] Ten pat.

Susirūpinusios, kad kabeliai nėra atsparūs šnipinėjimo ir sabotažui, kai kurios vyriausybės ėmė labiau saugoti savo teritorinius vandenis, netgi **užtęsti leidimų išdavimą kabelių tiesimui ir priežiūrai**. Pvz., Indonezija ir Kanada nustatė, kad tik tam tikri laivai gali tiesti ir prižiūrėti kabelius jų išskirtinėse ekonominėse zonose.[42]

Pagal ilgalaikius techninio aptarnavimo susitarimus svarbiausią kai kurių šalių infrastruktūrą dažnai prižiūri šalys, kurios nebūtinai yra draugiškos infrastruktūros savininkams. Pvz., 2022 m. sugedusį pagrindinį tarpžemyninį šviesolaidinį kabelį, priklausantį JAV kompanijoms AT&T ir „Verizon", remontavo kinų inžinieriai, dirbę Kinijos laive. Tais pačiais metais tas pats laivas Rytų Kinijos jūroje taisė kabelį, priklausantį „Microsoft" ir Japonijos telekomunikacijų grupei „SoftBank".[43]

Pasak specialistų, kalbant apie įsilaužimo riziką, kabeliai labiausiai pažeidžiami atliekant jų techninį aptarnavimą – darbų metu **gali būti įterpti tam tikri įrenginiai, skirti perduodamiems duomenims kopijuoti ar netgi iškraipyti**. Gaminant ar taisant kabelius įmanoma įterpti duomenų nuskaitymo įrenginius į vadinamuosius *kartotuvus* (elektroninius komponentus, jungiančius skirtingas kabelių dalis, kad stiprumo nepraradęs signalas nukeliautų ilgesnį atstumą).

Vis dėlto, svarbiausias tarptautinis Kinijos interesas yra ekonominis, todėl jai nebūtų naudinga griauti savo reputaciją. Atsižvelgdami į tai, kai kurie ekspertai yra linkę manyti, kad Pekinas neturi rimtų motyvų rengti diversijas ir organizuoti plataus masto kibernetinį kenkimą.

Kinija – ne vienintelė šalis, kurios stambiausios technologijų įmonės bendradarbiauja su valstybine administracija atliekant žvalgybą užsienyje. Kai kurios JAV technologijų milžinės taip pat pasitelkia savo tinklus, kad **palengvintų Jungtinėms Valstijoms stebėjimą, šnipinėjimą ir gynybos operacijas**. Kita vertus, daugelis vyriausybių turi aiškias nacionalines nuostatas dėl stebėjimo, dirbtinio intelekto infrastruktūros ir kitų technologijų, kurios galėtų pažeisti stebimų asmenų privatumą ar atskleisti organizacijų komercines paslaptis.[44]

Nemažą grėsmę kabelių fiziniam ir kibernetiniam saugumui kelia Kinijos įmonių dominavimas kabelių remonto rinkoje. Pvz., valstybės kontroliuojama Kinijos bendrovė „S.B. Submarine Systems" taiso tarptautinius povandeninius kabelius, įskaitant JAV kompanijoms, tarp kurių – „Google" ir „Meta", priklausančias linijas. Nerimaujama, kad tokios kinų bendrovės gali „nuskaityti" povandeninius duomenų srautus, susidaryti vandenyno dugne nutiestų JAV karinių jungčių žemėlapius, taip pat iš techninės kabelių sistemos dokumentacijos sužinoti labai konkrečią informaciją, kuri karo atveju leistų greitai ir tiksliai nukirsti linijas. Be to, pernelyg pasikliaujant kinų techninio aptarnavimo laivais rizikuojama, kad karinio konflikto atveju Kinijos Vyriausybė uždraustų juos naudoti, ir povandeniai kabeliai kurį laiką nebūtų taisomi.[45]

Viešojo diskurso analizė leidžia teigti, kad tarptautinė bendruomenė, ypač – JAV, atsižvelgia į povandeninei infrastruktūrai Kinijos keliamas grėsmes. Pateikiama ir įvairių rekomendacijų, pvz., supaprastinti JAV verslo subjektams leidimų tiesti ir prižiūrėti kabelius išdavimą, sukurti lengvatinių

[42] Gross, A., Heal, A. Campbell, C. Clark, D., Bott, I., De la Torre Arenas, I. (2023 m. birželio 13 d.). How the US is pushing China out of the internet's plumbing. Prieiga per internetą: *https://ig.ft.com/subsea-cables/*
[43] Ten pat.
[44] Ten pat.
[45] Runde, D., Murphy, E., Bryja T. (2024 m. rugpjūčio 16 d.). Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition. Prieiga per internetą: *https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition*

kreditų tokiai veiklai sistemą, plėtoti amerikietišką kabelių remonto laivyną, siekti didesnės tarptautinės atsakomybės už kabelių gadinimą.[46]

6. Kiniškų technologijų skverbimasis į Lietuvą

Kinijos technologijų Lietuvai keliami pavojai – ne nauja tema šalies viešojoje erdvėje. Šiame skyriuje primenami keli plačiau diskutuoti atvejai pradedant naujausiais.

2025 metų vasarį Lietuvos Seimo kanceliarija **uždraudė parlamentarams ir Seimo darbuotojams išduotuose kompiuteriuose bei telefonuose naudoti Kinijoje sukurtą DI įrankį „DeepSeek"**.[47]

2025 m. Kinijos pristatyta programa „DeepSeek" prieinama už mažesnę kainą ir konkuruoja su geriausiais JAV DI modeliais, tačiau, kilus įtarimams, kad „DeepSeek" gali perduoti užsiregistravusių vartotojų duomenis Kinijos valstybinei telekomunikacijų įmonei, dalis Vakarų šalių pradėjo svarstyti galimybę riboti prieigą prie šios programos.[48]

2021 metų kovą Valstybės saugumo departamentas kartu su Antruoju operatyvinių tarnybų departamentu prie Krašto apsaugos ministerijos pateikė grėsmių nacionaliniam saugumui vertinimą. Valstybės saugumo departamento vadovas Darius Jauniškis konstatavo, kad jo žinyba fiksavo ypatingą Kinijos kompanijos susidomėjimą vienos įmonės Lietuvoje vykdomu išmaniosios infrastruktūros diegimo konkursu. Neįvardyta Kinijos kompanija pasiūlė nemokamai sumontuoti nemažą dalį projektui reikalingos įrangos. Pasak Jauniškio, tikėtina, kad taip **buvo siekiama ne tik tiekti įrangą ir technologijas, bet ir „įlįsti į įmonės vidų ir susipažinti su įmonės operaciniais technologiniais procesais, kibernetinės informacijos saugos reikalavimais".**[49]

2021 m. tuometinis Seimo nacionalinio saugumo ir gynybos komiteto vadovas Laurynas Kasčiūnas išsakė nuomonę, kurią glaustai galima išreikšti taip: „Lietuvos viešųjų pirkimų sistemoje dominuojantis **mažiausios kainos principas leidžia biudžetinėms organizacijoms nepažeidžiant galiojančių teisės aktų pirkti kibernetinio ir nacionalinio saugumo spragų turinčius prietaisus**".[50]

Duomenų apsaugos prasme nepatikimų technologijų sfera aprėpia ir buityje bei versle naudojamą įrangą. Pristatydamas 2019 m. kibernetinio saugumo ataskaitą tuometinis krašto apsaugos viceministras Edvinas Kerza perspėjo, kad Lietuvoje ir visame pasaulyje plačiai naudojama tariamai kiniška ar kitose Azijos šalyse pagaminta įranga iš tiesų gali būti rusiška. Per ją galima šnipinėti gyventojus ir įmones.[51]

[46] Ten pat.
[47] Jaruševičiūtė-Mockuvienė, G. (2025 m. vasario 13 d.). Seimo įrenginiuose uždrausta naudoti Kinijoje sukurtą DI programėlę „DeepSeek". Prieiga per internetą: *https://www.bernardinai.lt/seimo-irenginiuose-uzdrausta-naudoti-kinijoje-sukurta-di-programele-deepseek/*
[48] Ten pat.
[49] Joana Lapėnienė, J. (2021 m. kovo 7 d.). Lietuvos ir kaimyninių šalių žvalgybos perspėja – Kinija siekia sukurti sistemą, kur visi veiktų pagal Pekino standartus. Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/1359658/lietuvos-ir-kaimyniniu-saliu-zvalgybos-perspeja-kinija-siekia-sukurti-sistema-kur-visi-veiktu-pagal-pekino-standartus*
[50] Jockus, A. (2021 m. balandžio 9 d.). Kaina prieš saugumą: kokią IT įrangą turėtų pirkti viešasis sektorius? Prieiga per internetą: *https://www.alfa.lt/verslo-naujienos/kaina-pries-sauguma-kokia-it-iranga-turetu-pirkti-viesasis-sektorius/-50442012/*
[51] Jačauskas, I. (2020 m. balandžio 16 d.). Gyventojų masiškai naudojama kiniška ir rusiška įranga gali juos šnipinėti? Prieiga per internetą: *https://kauno.diena.lt/naujienos/lietuva/salies-pulsas/gyventoju-masiskai-naudojama-kiniska-ir-rusiska-iranga-gali-juos-snipineti-962747*

Analitinių apžvalgų archyvas: *https://lnb.lt/istekliai/kiti-istekliai/analitines-apzvalgos*

Pasak Kerzos, Nacionalinio kibernetinio saugumo centro specialistai fiziškai ištyrę vieną iš populiariausių namuose naudojamų belaidžio tinklo maršrutizatorių nustatė, kad jis siunčia duomenis į serverius Rusijoje. Reaguodama į tai, kad Taivane, Kinijoje ir Rusijoje pagaminta elektronika neatitinka saugumo standartų, ES nurodė institucijoms parengti sertifikavimo schemas – bet kuriam prie interneto jungiamam įrenginiui, kurį norima platinti ES, kuri nors bendrijos valstybė turės išduoti sertifikatą. Kaip teigė Kerza, 90 proc. Lietuvoje naudojamų belaidžių maršrutizatorių yra pagaminti Kinijoje arba Taivane, tačiau pasitaiko atvejų, kai tariamai taivanietiški produktai išties yra pagaminti Rusijoje.[52]

2019 metų pradžioje keli parlamentarai kreipėsi į specialiąją Vyriausybės komisiją prašydami įvertinti **rizikas dėl Kinijos informacinių technologijų milžinės „Huawei" įrangos ir Lietuvoje diegiamo 5G ryšio**, taip pat pateikti išvadas ar rekomendacijas, ar nevertėtų naudoti tik europietiškų ar NATO šalių technologinių produktų. Seimo nariai rėmėsi JAV įsikūrusio Strateginių ir tarptautinių studijų centro 2018 metų ataskaitoje pateikta informacija, kad kompanijos „Huawei" ir ZTE buvo subsidijuojamos Kinijos Vyriausybės, kad įgytų stiprias pozicijas rinkoje ir žvalgybinį pranašumą. Tuometis Nacionalinio kibernetinio saugumo centro vadovas Rytis Rainys sakė, kad jokių „Huawei" įrangos kenkėjiškos veiklos faktų nenustatyta, „kad būtų galima pateikti konkrečias rekomendacijas ar išvadas. Tačiau situacija dinamiška ir rūpestį kelia įvairūs pranešimai iš kitų pasaulio šalių".[53] 2019 metų gegužę naujienų agentūra „Reuters" pranešė, kad kovą su tuomet premjero pareigose dirbusiu Sauliumi Skverneliu susitikusi JAV ambasadorė Anne Hall spaudė Lietuvos Vyriausybę atsisakyti „Huawei" dalyvavimo plėtojant 5G tinklą Lietuvoje. Žiniasklaidos duomenimis, „JAV ambasadorė ragino imtis veiksmų dėl „Huawei" ir sakė, kad dėl šios bendrovės 5G ryšio įrangos NATO sąjungininkų kariai gali tapti pažeidžiami". Apie „Reuters" pranešimą informuojančioje lietuviškoje publikacijoje rašyta, kad „Vyriausybės atstovai iki šiol teigė neturintys priežasčių uždrausti „Huawei" įrangos naudojimą civiliniais tikslais, bet [tuometinis] krašto apsaugos ministras Raimundas Karoblis pareiškė, kad krašto apsaugos sistemoje „Huawei" technologijų nebus".[54]

Apibendrinant galima teigti, kad Kinijos įmonių, kiniškų technologijų skverbimąsi į Lietuvą stebi įgaliotos šalies žinybos, o saugos priemonių efektyvumas išryškės įvykus rimtesniems technologiniams įsilaužimams.

7. Apibendrinimas ir akcentai, į ką atkreipti dėmesį ateityje

Povandeniniai ryšio kabeliai sudaro globalizuotos, skaitmena paremtos pasaulinės ekonomikos informacinį karkasą, kuriam šiuo metu nėra ir greitu laiku neatsiras alternatyvos.

[52] Ten pat.
[53] Naprys, E. (2019 m. sausio 29 d.). Seimo nariai susirūpinę dėl „Huawei" – kreipėsi ir į vyriausybės komisiją. Prieiga per internetą: *https://www.lrt.lt/naujienos/verslas/4/243053/seimo-nariai-susirupine-del-huawei-kreipesi-ir-i-vyriausybes-komisija?srsltid=AfmBOorYAoDRrE1e2lKDc8KpVnz8Z_sC0DfcjoEBoOfFKWNB_JFxtmAh*
[54] Beniušis, V. (2019 m. gegužės 24 d.). „Reuters": JAV ambasadorė spaudė Lietuvos Vyriausybę dėl „Huawei". Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/1062639/reuters-jav-ambasadore-spaude-lietuvos-vyriausybe-del-huawei?srsltid=AfmBOool9Yy7vx1xBlXGGqpCbZ7a83A3NnQzb4ZZqX-8fJDsUx-ezwPC*

Analitinių apžvalgų archyvas: *https://lnb.lt/istekliai/kiti-istekliai/analitines-apzvalgos*

Kinija deda daug pastangų, kad įsitvirtintų pasaulinėje povandeninių kabelių tiesimo ir remonto rinkoje. Nuogąstaujama, kad ši valstybė, pasinaudodama kabelių techninės priežiūros paslaugų teikėjos vaidmeniu, gali diegti kabelių infrastruktūroje šnipinėjimo įrangą.

Kinijos vykdoma skaitmeninių technologijų plėtra turi ir politinį aspektą. Vadinamoji „Skaitmeninio šilko kelio“ iniciatyva („Vienos juostos, vieno kelio“ iniciatyvos dalis) pasitelkiama siekiant Kinijos paramą gaunančioms šalims įpiršti kiniškomis technologijomis pagrįstą autoritarizmo modelį. Kinijos technologijų įmonės jau padėjo kitų šalių vyriausybėms kurti ir diegti stebėjimo įrangą, kuri gali būti panaudota prieš opozicines jėgas. Pagal Kinijos kibernetinio saugumo įstatymus, net ir privačios įmonės privalo saugoti duomenis šalies teritorijoje esančiuose serveriuose, taigi tie duomenys gali būti prieinami Kinijos valdžios institucijoms.

Tarptautinė bendruomenė, ypač – JAV, atsižvelgia į povandeninei infrastruktūrai Kinijos keliamas grėsmes. Pateikiama ir įvairių rekomendacijų, pvz., supaprastinti JAV verslo subjektams leidimų tiesti ir prižiūrėti kabelius išdavimą, sukurti lengvatinių kreditų tokiai veiklai sistemą, plėtoti amerikietišką kabelių remonto laivyną, siekti didesnės tarptautinės atsakomybės už kabelių gadinimą.

Rusija daug mažiau priklausoma nuo povandeninių kabelių nei JAV ar Kinija, nes yra žemyninė valstybė. Ji mažiau pažeidžiama dėl povandeninės infrastruktūros sutrikimų, galbūt todėl yra labiau linkusi išnaudoti kitų šalių pažeidžiamumą šioje srityje.

Apibendrinant galima teigti, kad Kinijos įmonių, kiniškų technologijų skverbimąsi į Lietuvą stebi įgaliotos šalies žinybos, o saugos priemonių efektyvumas išryškės įvykus rimtesniems technologiniams įsilaužimams.

Akcentai, į ką atkreipti dėmesį ateityje

- Lietuvos valdžios institucijos suvokia kritinės infrastruktūros svarbą, todėl būtina stiprinti jau vykdomas infrastruktūros apsaugos priemones.

- Svarbu stiprinti kooperaciją ES saugos standartų, taikomų skaitmeninėms technologijoms (visų pirma ne ES kilmės), tobulinimo srityje.

- Atsižvelgiant į tai, kad dabar egzistuojanti jūrų teisė dėl kintančių technologinių sąlygų ne visada pritaikoma infrastruktūros gadinimo atvejams, Lietuva galėtų prisidėti prie egzistuojančių tarptautinių normų tobulinimo.