

Hibridinio karo poveikis civiliniams teisiniams santykiams

Titas Mikalauskas

Vilniaus universiteto Teisės fakulteto
IV kurso, Privatinė teisė: civiliniai ginčai šakos studentas
Saulėtekio al. 9, I rūmai, 10222 Vilnius
El. paštas: titas.mikalauskas@tf.stud.vu.lt

Domas Adolfas Gylis

Vilniaus universiteto Teisės fakulteto
V kurso, Privatinė teisė: civilinė ir verslo teisė šakos studentas
Saulėtekio al. 9, I rūmai, 10222 Vilnius
El. paštas: domas.gylis@tf.stud.vu.lt

Mokslinio straipsnio akademinė kuratorė dokt. Deimantė Rimkutė

El. paštas: deimante.rimkute@tf.vu.lt

Santrauka. Šiuo straipsniu siekiama ištirti galimą hibridinio karo poveikį civiliniams teisiniams santykiams. Išskirtinos keturios aktualios hibridinio karo priemonių grupės: dezinformacijos kampanijos, kibernetinės atakos, diversinės atakos ir kitos priemonės. Nagrinėjant dezinformacijos kampanijų poveikį, pastebėta, kad dezinformacinės kampanijos gali sudaryti prielaidas pažeisti asmenų garbę ir orumą, kas lemtų didesnę CK 2.24 straipsnyje numatytų gynybos būdų taikymą, taip pat gali pabloginti komercinių subjektų reputaciją. Kalbant apie kibernetines atakas, išskirta, kad jos apsunkina galimybes nustatyti žalą padariusį asmenį. Diversinių atakų analizė parodė, kad sabotazas lemia valstybės reguliavimo griežtėjimą ir didina privačių subjektų pareigą aktyviau užtikrinti savo infrastruktūros saugumą. Kitos hibridinio karo priemonės, nors ir sunkiai sistemškai apibrėžiamos, akivaizdžiausiai pasireiškia transporto sektoriuje ir kelia skirtingus valstybės atsakomybės bei rizikos paskirstymo klausimus.

Pagrindiniai žodžiai: civilinė teisė, civiliniai teisiniai santykiai, hibridinis karas, hibridinio karo poveikis.

Summary. This article aims to examine the potential impact of hybrid warfare on civil legal relations. Four relevant groups of hybrid warfare measures are distinguished: disinformation campaigns, cyberattacks, diversionary attacks, and other measures. In analyzing the impact of disinformation campaigns, it was observed that such campaigns may create pre-

conditions for violations of individuals' honor and dignity, which would lead to increased application of the remedies provided for in Article 2.24 of the Civil Code, and may also harm the reputation of commercial entities. With regard to cyberattacks, it was noted that they complicate the identification of the person who caused the damage. The analysis of diversionary attacks showed that sabotage leads to stricter state regulation and increases the obligation of private entities to more actively ensure the security of their infrastructure. Other hybrid warfare measures, although difficult to define systematically, manifest most clearly in the transport sector and raise different issues of state liability and risk allocation.

Keywords: *civil law, civil legal relations, hybrid warfare, impact of hybrid warfare.*

Įvadas

Temos aktualumas. Vis didėjant visuomeninei pažangai komunikacijos, mokslo, technologijų ir kitose srityse, kartu keičiasi ir konfliktas. Mums visiems žinoma, kad svarbūs karo elementai - ginklai ir taktika - istoriškai buvo nuolat keičiami, siekiant prisitaikyti prie tuometinio konteksto, kad būtų galima priešą priversti paklusti jėga. Vis dėlto šiomis dienomis tokį karą (karybą) jau galime vadinti tradiciniu, nes pastarųjų dešimtmečių technologiniai ir visuomeniniai pokyčiai padėjo atsirasti naujo tipo karui, paprastai vadinamam hibridiniu. Hibridinio karo sąvoka stokoja apibrėžtumo, tačiau viešojoje erdvėje tai dažniausiai apibūdinama per nereguliarią, t. y. neįprastą, taktiką: kibernetines atakas, informacines atakas (propagandą), provokacijas, sabotажą ir kitą, kuria būtų galima pasinaudoti siekiant politinių tikslų. Pavyzdžiui, kibernetinėmis atakomis gali būti siekiama pakenkti civilinei infrastruktūrai, taip destabilizuojant pačią visuomenę, o per informacines atakas – skatinti nepasitikėjimą ir susikiršinimą visuomenėje. Tokios taktikos neabejotinai gali paveikti ir privačių asmenų teisinius santykius. Pavyzdžiui, kibernetinės ir diversinės atakos kelia iššūkių dėl atsakingo asmens nustatymo bei valstybės netiesioginės atsakomybės, o informacinės atakos – gali daryti įtaką asmenų reputacijai.

Atsižvelgiant į tai, kad civiline teise siekiama sureguliuoti privačių fizinių ir juridinių asmenų tarpusavio santykius, neišvengiamai kyla klausimas apie hibridinio karo poveikį šiems santykiams. Tai ypatingai aktualu dėl trijų priežasčių. Pirma, turint mintyje, kad tai yra karyba, išsiskirianti savo nereguliarumu, gali kilti klausimas ar šiandieninė civilinė teisė yra tam pasirengusi. Nereguliari taktika gali atverti naujas spragas teisiniame reguliavime ir subjektų elgesyje, ką būtinai reikėtų ištirti. Antra, yra tvirtas pagrindas manyti, kad privatūs subjektai yra pagrindiniai tokios karybos taikiniai. Daugelyje šalių vyraujant rinkos ekonomikai, tikėtina, kad privačių subjektų atžvilgiu bus taikomi hibridinio karo metodai. Trečia, hibridinis karas daro karo ir taikos ribas mažiau ryškias. Karo ir taikos apibrėžtumo stoka gali lemti nestabilumo jausmą, kas gali keisti subjektų elgesį.

Taigi, atsižvelgiant į tai, kad hibridinis karas gali civiliniams teisiniams santykiams iškelti naujų iššūkių, t. y. išryškinti spragas teisiniam reguliavime, paveikti subjektus ir lemti kitokį jų elgesį, sukurti nestabilią aplinką tokiems santykiams vystytis, būtina giliau ištirti galimą tokios karybos poveikį. Išsamesnis poveikio tyrimas gali padėti tobulinti civilinių teisių santykių reglamentavimą, kad būtų galima apsaugoti šių santykių apyvartą nuo neigiamų pasekmių.

Darbo objektas. Tai yra hibridinio karo priemonių reikšmė civiliniams teisiniams santykiams Lietuvos Respublikoje. Šiame darbe dėmesys telkiamas į konkrečias hibridinio karo priemones ir jų savybes, siekiant nustatyti, kokias teises pasekmes jos gali sukelti civilinės teisės reguliuojamiems santykiams. Šis darbas grindžiamas prielaida, kad skirtingos hibridinio karo priemonės pasižymi nevienodu veikimo mechanizmu, todėl jų sąveika su civilinės teisės institutais taip pat nėra vienoda. Dėl šios priežasties darbo centre yra ne abstraktus hibridinio karo poveikis privatiems santykiams, bet konkrečių hibridinio karo priemonių nulemti teisiniai klausimai ir iššūkiai civilinės teisės reguliavimui.

Tyrimo ribos apibrėžiamos atsižvelgiant į šiame darbe pasirinktą hibridinio karo sampratą. Kadangi šiame darbe hibridinis karas suprantamas kaip veikimas neperžengiant karo slenksčio tradicine prasme, jo reikšmė analizuojama taikant bendrąjį civilinės teisės režimą taikos metu. Todėl darbe nesiekama tirti teisių padarinių, kylančių iš specialiųjų karo meto režimų ar ginkluoto konflikto aplinkybių. Taip pat tyrimas nėra orientuotas į bendruosius prievolių vykdymo kliūčių atvejus (t. y. *force majeure* ir *rebus sic stantibus*), nes tokios pasekmės gali kilti dėl įvairių išorinių veiksnių ir savaime neatskleidžia hibridinio karo priemonių specifikos. Šiame darbe aktualus būtent tas poveikis, kuris kyla iš konkrečios hibridinio karo priemonės pobūdžio ir leidžia vertinti jos reikšmę civilinės teisės institutų veikimui.

Darbo tikslas. Šiame darbe siekiama nustatyti, kaip skirtingos hibridinio karo priemonės gali paveikti privačių subjektų turinius, neturinius ir kitus civilinius teisinius santykius bei kokius iššūkius toks poveikis gali kelti teisiniui reguliavimui.

Darbo uždaviniai.

- Apibrėžti hibridinio karo sąvoką, taip sukuriant sąlygas tolimesniam temos nagrinėjimui;
- Išskirti Lietuvai aktualias hibridinio karo priemones (jų grupes), kurios gali daryti poveikį civiliniams teisiniams santykiams;
- Išnagrinėti hibridinio karo poveikį aktualioms civilinių teisių santykių sritims;
- Esant galimybei, pasiūlyti priemones reaguoti į hibridinio karo poveikį atitinkamuose civilinės teisės institutuose.

Tyrimo metodai.

- Abstrakcijos. Abstrakcijos tyrimo metodu siekiama tyrimą atriboti nuo mažiau aktualių, neesminių dalykų. Pavyzdžiui, šis metodas taikomas išskirti aktualias hibridinio karo priemones, kurių poveikis toliau nagrinėjamas.

- Doktrininis. Doktrininis tyrimo metodas šiame darbe pasitelkiamas siekiant aiškinti tam tikrus civilinių teisinių santykių institutus bei jų veikimą, taip pat darbui aktualias sąvokas.
- Analizės. Šis tyrimo metodas derinamas kartu su doktrininio tyrimo metodu siekiant išnagrinėti konkrečių hibridinio karo priemonių poveikį civiliniams teisinių santykių institutams.

Hibridinis karas

Hibridinio karo sąvoka

Hibridinio karo sąvoką pirmą kartą 2007 m. panaudojo Frank Hoffman. Tuo metu jis teigė, kad hibridiniai karai apima įvairius karo veiksmų būdus, įskaitant konvencinius pajėgumus, nereguliuojamas taktikas ir formacijas, teroristinius veiksmus, įskaitant beatodairišką smurtą ir prievartą bei nusikalstamą elgesį¹. Taigi, Hoffman pateiktoje sampratoje hibridinis karas apima tiek kinetines, tiek nekinetines priemones, tačiau pagrindinis vaidmuo tenka konvencinėms kinetinėms priemonėms, t. y. jėgos panaudojimui. Nekinatinės priemonės čia atlieka pagalbinę funkciją. Pažymėtina, kad šiuo aspektu vėlesni autoriai pateikia skirtingus apibrėžimus.

Pavyzdžiui, Andrew Mumford ir Pascal Carlucci teigia, kad hibridinis karas apibrėžiamas sinchroniniu kinetinių ir nekinetinių priemonių naudojimu siekiant galutinių politinių tikslų². Pavyzdžiui, žiniasklaidoje vis dažniau pasirodo publikacijų, kuriose hibridinis karas išimtinai apibrėžiamas per nekinetinių priemonių naudojimo prizmę³, o mokslinėje literatūroje pastebimi teiginiai, kad hibridinio karo apibrėžimui kinetinės priemonės (juo labiau konvencinės) net iš viso nėra būtinos⁴. Taigi, matome, kad hibridinio karo sąvoka neturi vieningo, visuotinai pripažinto apibrėžimo. Tai įvertinus, galima pripažinti, kad, siekiant nustatyti hibridinio karo poveikį civiliniams teisiniams santykiams, būtina pateikti sąvoką, kuria pasitelksime toliau atliekant tyrimą.

Šio darbo autorių nuomone, hibridinis karas turėtų būti suvokiamas kaip įvairių (kombinuotų) kinetinių ir nekinetinių priemonių naudojimas nepereinant į karo stadiją konvencine (tradicine) prasme. Tai reiškia, kad hibridinis karas gali vykti ir mums įprastai suvokiamu taikos metu, kai tam tikri politiniai dariniai nereguliais

¹ HOFFMAN G., Frank (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, psl. 14.

² MUMFORD, Andrew ir CARLUCCI, Pascal (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, 8(2), psl. 192-206.

³ GOTEV, Georgi (2021-10-28). The Brief, powered by Facebook – Hybrid warfare [interaktyvus]. Prieiga per internetą: <https://www.euractiv.com/opinion/the-brief-powered-by-facebook-hybrid-warfare/>.

⁴ BARGAOANU, Alina ir NEGREA-BUSUIOC, Elena (2024-06-21). *Hybrid Warfare is Less Than Warfare: A Dangerous Illusion* [interaktyvus]. https://irregularwarfarecenter.org/wp-content/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf.

metodais siekia politinių tikslų, tačiau vengia atviro konflikto. Taigi, hibridinį karą reikėtų atriboti nuo karo konvencine prasme, t. y. išskirti į atskirą karo rūšį. Toks atribojimas svarbus ir teisiniu požiūriu. Istorikai tiek nacionalinė teisė, tiek tarptautinė viešoji teisė buvo grindžiamos gana aiškiu karo ir taikos būsenų atskyrimu, nuo kurio priklausė skirtingų teisinių režimų taikymas. Vis dėlto technologinė ir socialinė raida sudarė prielaidas atsirasti veiksams, kurie savo poveikiu prilygsta priešiška veiklai, tačiau formaliai neperžengia karo slenkščio. Tai atskleidžia teisėkūrai būdingą problemą – teisinis reguliavimas neretai prisitaiko prie naujų visuomeninių reiškinių lėčiau, nei jie susiformuoja praktikoje.

Šiame darbe pateikiamas hibridinio karo apibrėžimas išskiriamas dėl dvejų priežasčių. Pirmą, būtų neprotinga teigti, kad visuomenei taip smarkiai pasikeitus socialine ir technologine prasme, tam tikros apraiškos, kurios vadintinos hibridiniu karu, vis tiek turėtų būti neatsiejamos nuo konvencinio karo. Atkreiptinas dėmesys, kad minėtos apraiškos veikia kitaip ir, žinoma, daro kitokį poveikį nei konvenciniai karo būdai. Konvencinė karyba siekia atviromis ir kinetinėmis priemonėmis priversti paklusti, o hibridinė karyba yra ženkliai subtilesnė. Antra, hibridinio karo neišskyrimas į atskirą karo rūšį neatitiktų šiandieninių geopolitinių tendencijų. Rusijos Federacijos hibridinio karo doktrinoje dažnai užsimenama apie nekonvencinę hibridinio karo prigimtį, kuri, be kita ko, labiausiai siejama su informaciniu karu⁵. Taip pat pabrėžtina, kad hibridinio karo samprata nėra lengvai suderinama su tradicinėmis tarptautinės viešosios teisės maksimomis, grindžiamomis aiškiu karo ir taikos atribojimu, valstybių suvereniteto apsauga bei jėgos nenaudojimo principu, nes hibridinės priemonės dažnai veikia šių kategorijų „pilkojoje zonoje“.

Viską apibendrinus, galime teigti, kad hibridinio karo sąvoka turi daug apibrėžimų, todėl toliau atliekant tyrimą būtina suformuluoti hibridinio karo sąvoką. Manome, kad hibridinis karas turėtų būti apibrėžiamas kaip įvairių (kombinuotų) kinetinių ir nekinetinių priemonių naudojimas nepereinant į karo stadiją konvencine (tradicine) prasme. Matome, kad apraiškos, priskirtinos hibridinio karo apibrėžimui, yra pernelyg besiskiriančios nuo konvencinio karo apraiškų ir todėl turėtų būti atskirtos nuo konvencinio karo apibrėžimo. Atsižvelgiant į tai, tikslingiausia kalbėti apie hibridinio karo poveikį būtent taikos metu (konvencinio karo prasme), nes tokiu būdu galime tiksliau ištirti būtent hibridinio karo poveikį civiliniams teisiniams santykiams.

Hibridinio karo priemonės

Taigi, apibrėžus hibridinio karo sąvoką, būtina išskirti kinetines ir nekinetines priemones, apie kurių poveikį kalbėsime ir kurios aktualiausias Lietuvos kontekste.

⁵ FRIDMAN, Ofer (2018). *Russian 'Hybrid Warfare'. Resurgence and Politicisation*. New York: Oxford University Press, p. 75-90.

Manome, kad tikslinga išskirti hibridinio karo priemonės į keturias grupes: dezinformacijos kampanijas, kibernetines atakas, diversines atakas ir kitas priemones. Toliau aptarsime kiekvieną iš šių grupių.

Kalbant apie dezinformacijos kampanijas, tai jau buvo minėta, kad Rusijos Federacijos hibridinio karo doktrinoje informacinis karas atlieka svarbų vaidmenį. Tokie veiksmai dažniausiai įvardijami kaip informacijos manipuliacijos ir kišimasis iš užsienio (toliau - FIMI, angl. Foreign Information Manipulation and Interference)⁶. Žinoma, FIMI veiksmai neapsiriboja pačia dezinformacija, tačiau jos vaidmuo šiuose veiksmuose pats svarbiausias. Ja sąmoningai siekiama deorganizuoti visuomenę, dinti joje susipriešinimą. Tai ypatingai aktualu atsižvelgiant į tai, kad, remiantis Kylio instituto duomenimis, Lietuva yra viena iš labiausiai remiančių Ukrainą valstybių vertinant proporcingai pagal kiekvienos šalies bendrąjį vidaus produktą⁷.

Kibernetinės atakos, ko gero, yra pačios pavojingiausios hibridinio karo priemonės, ypatingai turint mintyje šiandieninės visuomenės priklausomumą nuo informacinių technologijų. Jomis gali būti kėsinamasi į tam tikrus svarbius duomenis (komercines paslaptis, asmens duomenis), infrastruktūrą, nuosavybę (kriptoturtą, pinigus), saugumą, paslaugų prieinamumą ir į kitas sritis, kurios svarbios visuomenei. Atsižvelgiant į tai, neabejotina, kad kibernetinėmis atakomis sukelinta žala gali būti milžiniška. Ši hibridinio karo priemonė yra svarbi ne tik Lietuvos kontekste, bet ir viso NATO. Pavyzdžiui, pastaruoju metu kibernetinių atakų atvejų prieš NATO valstybes vis daugėja⁸.

Hibridinio karo kontekste pastaruoju metu vis dažniau pastebimos ir diversinės atakos (sabotažas), kurios pasireiškia kaip slapti, fizinį poveikį sukeliantys incidentai, sutrikdantys infrastruktūros veikimą ir sistemingai mažinantys valstybės atsparumą. Tradiciškai tokie veiksmai būdavo nukreipti į karinius objektus, tačiau pastaraisiais metais vis labiau matoma, kad sabotažo taikiniais tampa ir civilinė infrastruktūra. Ši dinamika ypač atsiskleidžia vertinant paskutiniuosius incidentus Europoje: 2023 m. pažeistas dujų vamzdynas „Balticconnector“ tarp Suomijos ir Estijos, 2024 m. užfiksuoti gaisrai keliuose DHL logistikos sandėliuose Vokietijoje, o 2024 m. gegužę kilęs gaisras Vilniaus „Ikea“ prekybos centre dar labiau išryškino nerimą keliančių „atsitiktinumų“ tendenciją. Atsižvelgiant į šias aplinkybes, matyti, kad sabotažas vis labiau įsivertina kaip nuolatinė grėsmė tiek Lietuvoje, tiek Europos Sąjungoje⁹.

⁶ European Union External Action (2025-03-14) *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)* [interaktyvus] https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#45330.

⁷ Kiel Institut (2025-10) *Ukraine Support Tracker Data* [interaktyvus] <https://www.kielinstitut.de/publications/ukraine-support-tracker-data-6453/>

⁸ The Guardian. *Russian cyber-attacks against NATO states up by 25% in a year, analysis finds*. [interaktyvus] <https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds>.

⁹ Irregular Warfare Initiative. *Sabotage as a "New Normal"*. [interaktyvus] <https://irregular-warfare.org/articles/sabotage-as-a-new-normal/>.

Kitos priemonės yra tokios hibridinio karo priemonės (veiksmai), kurių dėl savo specifikos (vienos priemonės savo esme kinetinės, o kitos – ne ir pan.) negalima arba pernelyg sunku priskirti prie konkrečios grupės. Pavyzdžiui, bepiločiai dronai gali būti pasitelkiami vykdyti diversines atakas, tačiau neretai jie būna naudojami visai kitais tikslais, kaip tam tikrų funkcijų trikdymas. Funkcijų trikdymui taip pat gali būti pasitelkiamas embargas, kontrabandiniai balionai, klaidinantys pranešimai apie galimą pavojų. Tai aktualu ir Lietuvoje, nes įvairiausių funkcijų trikdymo atveju vis daugėja.

Hibridinio karo poveikis

Dezinformacijos kampanijos

Civiliniuose teisiniuose santykiuose svarbu, kad informacija, kuria dalinamasi, būtų teisinga. Šiuo aspektu FIMI veiksmais skleidžiama klaidinga informacija, taip pakenkiant civilinių teisinių santykių stabilumui. Išskirtinos dvi civilinių teisinių santykių sritys, kuriose dezinformacija gali daryti didelį poveikį: santykiuose, susijusiuose su asmens garbe ir orumu ir sutartiniuose teisiniuose santykiuose.

Poveikis santykiuose, susijusiuose su asmens garbe ir orumu

Lietuvos Respublikos civilinio kodekso¹⁰ (toliau – CK) 1.114 straipsnyje numatyta, kad civilinė teisė saugo asmenines neturtines teises ir vertybes, t. y., be kita ko, asmens garbę ir orumą, taip pat jo dalykinę reputaciją. Šiuo atveju aktualus CK 2.24 straipsnis, kuriame numatyta aptariamų vertybių gynība. Pasakytina, kad asmenys turi pareigą nepaskleisti tikrovės neatitinkančių duomenų, kurie žemintų kito asmens garbę ir orumą ar juridinio asmens dalykinę reputaciją, o jei tokie duomenys paskleidžiami – nukentėjęs asmuo turi teisę reikalauti, kad tokie duomenys būtų panaikinti ir jam būtų atlyginta padaryta turtinė ir neturtinė žala. Kadangi FIMI veiksmai yra pasitelkiami vykdančią informacinį karą, yra pagrindo manyti, kad tokiu būdu yra sudaromos sąlygos asmenims lengviau pažeisti minėtą pareigą, kas gali lemti didesnę poreikį asmenims ginti savo teises pagal CK 2.24 straipsnį. Tai lemia dvi priežastys.

Pirma, viena iš FIMI priemonių – sąmoningas tikrovės neatitinkančios informacijos skleidimas. Tokia informacija pirmiausia siekiama supriešinti, skatinti tarpusavio nepasitikėjimą visuomenėje tiek tarp privačių asmenų, tiek santykių su valstybės institucijomis, kuo gali būti pasinaudota siekiant geopolitinių tikslų. Antra, FIMI pasireiškia sudėtingais manipuliacijos metodais, kurie apsunkina galimybę asmeniui atskirti teisingą informaciją nuo neteisingos. Tai reiškia, kad asmenys, klaidingai įsitikinę informacijos tikrumu, gali tapti jos platintojais.

¹⁰ Lietuvos Respublikos civilinis kodeksas. 2000 m. liepos 18 d. Nr. VIII-1864. *Valstybės žinios*, 2000, 74-2262.

Išsamiau aptariant šias dvi priežastis, pasakytina, kad Rusija, vykdamt informacinį karą, yra linkusi aktyviai skleisti ypatingai neigiamą požiūrį į Ukrainos valdžią ir ją remiančius asmenis (kaltinant juos korupcija ir pan.)¹¹. Atsižvelgiant į Lietuvos visuomenės veikėjų itin aktyvią paramą Ukrainai, tokia veikla gali sudaryti sąlygas jiems tapti FIMI veiksmų taikiniu. Pavyzdžiui, Lietuvos Aukščiausiąjame Teisme buvo nagrinėjama civilinė byla dėl Seimo nario Remigijaus Žemaitaičio tikrovės neatitinkančių teiginių, kad visuomenininkas Andrius Tapinas šalies pasienio apsaugai rinktas lėšas panaudojo azartiniais lošimams¹². Dėl analogiškų teiginių buvo nagrinėjama byla ir žurnalistės Rūtos Janutienės atžvilgiu¹³. Šiuo atveju nėra aišku, ar minėti asmenys buvo paveikti dezinformacijos kampanijos iš priešiškų valstybių, tačiau jų veiksmai buvo naudingi priešiškomis valstybėms. Tai aktualu ir turint mintyje tai, kad Rusijos Federacija vis dažniau vykdo verbavimo operacijas, kad paveikti asmenys skleistų jai naudingą naratyvą¹⁴.

Taigi, darytina išvada, kad FIMI veiksmai, kurie pasireiškia tikrovės neatitinkančios informacijos skleidimu, gali paveikti civilinius teisinius santykius, susijusius su asmens garbe ir orumu bei jo dalykine reputacija. Tokiu būdu palengvinama civilinių teisinių santykių subjektams skleisti tikrovės neatitinkančią informaciją.

Poveikis sutartiniuose teisiniuose santykiuose

Sutartiniai teisiniai santykiai grindžiami šalių tarpusavio pasitikėjimu ir bendradarbiavimu, todėl FIMI veiksmams skleidžiama tikrovės neatitinkanti informacija gali paveikti tiek sutarčių sudarymą, tiek jų vykdymą. Pastaraisiais metais dezinformacija vis dažniau naudojama prieš Vakarų šalių komercinius subjektus, siekiant menkinti jų reputaciją ir patikimumą. Pavyzdžiui, 2023 m. Rusija Afrikoje skleidė teiginius, kad JAV farmacijos įmonės, prisidengdamos vakcinų platinimu, naudojasi Afrikos gyventojais kaip „bandomaisiais triušiais“¹⁵. Literatūroje pastebima, kad tokio pobūdžio veiksmai jau yra pakenkę Vakarų šalių komercinių subjektų veiklai¹⁶.

¹¹ Atlantic Council (2024-02-29). *Undermining Ukraine: How Russia widened its global information war in 2023* [interaktyvus] <https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/>.

¹² Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus 2025 m. vasario 27 d. nutartis civilinėje byloje Nr. e3K-7-4-403/2025.

¹³ LRT. *Janutienė viešai paneigė apie „Laisvės TV“ ir Tapiną išsakytus žodžius* [interaktyvus]. <https://www.lrt.lt/naujienos/lietuvoje/2/2705463/janutiene-viesai-paneige-apie-laisves-tv-ir-tapina-issakytus-zodzius>.

¹⁴ LRT. *Rusijos Federacija stiprina įtakos operacijas Baltijos šalyse – verbuojamas jaunimas* [interaktyvus]. <https://www.lrt.lt/naujienos/pasaulyje/6/2749170/rusijos-federacija-stiprina-itakos-operacijas-baltijos-salyse-verbuojamas-jaunimas>

¹⁵ Wall Street Journal. *Russian Intelligence Is Pushing False Claims of U.S. Biological Testing in Africa, U.S. Says.* [interaktyvus] <https://www.wsj.com/world/africa/russian-intelligence-is-pushing-false-claims-of-u-s-biological-testing-in-africa-u-s-says-ea817592>.

¹⁶ BYMAN, Daniel (2025-03-20). *Foreign Malign Influence Targeting U.S. and Allied Corporations.* [interaktyvus] <https://www.csis.org/analysis/foreign-malign-influence-targeting-us-and-allied-corporations>.

Sutarčių sudarymo kontekste tokia informacija gali būti reikšminga, nes šalims svarbi kitos sutarties šalies reputacija ir patikimumas. Paskleista klaidinanti informacija apie tariamą sutartinių prievolių nevykdymą, netinkamą elgesį su darbuotojais ar kitus reputaciją menkinančius veiksmus gali lemti atsisakymą sudaryti sutartis tiek dėl praktinių, tiek dėl etinių priežasčių. Taigi, FIMI veiksmai gali pakenkti civilinių teisinių santykių subjektų reputacijai ir taip apsunkinti sandorių sudarymą.

Kibernetinės atakos

Civilinės atsakomybės samprata įtvirtinta CK 6.245 straipsnyje, kuriame ji apibrėžiama kaip turtinė prievolė atlyginti nuostolius ar sumokėti netesybas. Šiame straipsnyje šalia sutartinės išskiriama ir deliktinė civilinė atsakomybė, kuri siejama su žala, nesusijusia su sutartiniais santykiais. Manome, kad kibernetinės atakos deliktinės atsakomybės kontekste pirmiausia kelia iššūkių nustatant už žalą atsakingus asmenis, todėl šioje srityje kyla poreikis tobulinti teisinį reguliavimą.

Už žalą atsakingo asmens nustatymas

CK 6.263 straipsnio 2 dalis numato, kad žalą, padarytą asmeniui, turtui, o įstatymų numatytais atvejais – neturtinę žalą privalo visiškai atlyginti atsakingas asmuo. Taigi, šiuo atveju reikia nustatyti už žalą atsakingą asmenį. Jau minėta, kad kibernetinės atakos išsiskiria savo pavojingumu dėl to, kad šiandieninė visuomenė yra smarkiai integruota su informacinėmis technologijomis. Tai lemia, kad kibernetinėmis atakomis gali būti kėsinamasi į daugelį dalykų: nuosavybę, infrastruktūrą, saugumą ir kita. Pavojingumą stipriai didina ir tai, kad nustatyti žalą padariusį asmenį gali tapti ypatingai sunku. Kibernetinės atakos pasižymi tuo, kad jos gali būti vykdomos ne tam tikroje vietoje ir ne tam tikru laiku, o „nuotoliu“, taip pat jų vykdymui (juo labiau - ištyrimui) reikalingos specialiosios žinios. Be to, kibernetinių atakų kontekste dažnai susiduriama su situacijomis, kai žala padaroma ne vieno, o kelių asmenų veiksmais arba pasitelkiant sudėtingas technines priemones, automatizuotas sistemas ar tarpininkus. Tai dar labiau apsunkina žalą padariusio asmens identifikavimą. Gali kilti klausimų, ar už padarytą žalą atsako pats kibernetinę ataką įvykdęs asmuo, ar, pavyzdžiui, informacinių sistemų savininkas, paslaugų teikėjas ar kitas asmuo, kurio veikla ar neveikimas sudarė sąlygas tokiai žalai atsirasti. Atkreiptinas dėmesys ir į tai, kad kibernetinės atakos, kaip hibridinio karo priemonės, yra pasitelkiamos būtent priešiškų valstybių. Valstybės, siekiančios geopolitinių tikslų, dažnai naudojasi apsunkintomis galimybėmis nustatyti už tokias atakas atsakingus asmenis. Taigi, dažnai yra pasitaikę atvejų, kai tam tikros politinio pobūdžio atakos būna atsekamos iki priešiškų valstybių, tačiau šios atsakomybę neigia¹⁷.

¹⁷ SCHULZKE, Marcus. (2018). The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. *Perspectives on Politics*, 16(4), 954–968.

Taigi, kibernetinių atakų sukelta žala kelia iššūkių šiandieniniam deliktinės atsakomybės reglamentavimui, kuris paprastai grindžiamas aiškiai identifikuojamu žalą padariusiu asmeniu ir jo veiksmais. Kadangi tokias atakas dažnai gali vykdyti ar remti galingi subjektai, įskaitant valstybes, jų sukelta žala gali būti milžiniška, sunkiai išvengiama, o atsakingų asmenų nustatymas – itin sudėtingas arba apskritai neįmanomas.

Valstybės civilinė atsakomybė

Atsižvelgiant į tai, kad už kibernetinę ataką atsakingus asmenis sunku nustatyti, didelę reikšmę įgyja deliktinės atsakomybės taikymo valstybei galimybių klausimas. Šiuo aspektu tikslingiausia kalbėti apie valstybės, kurioje žala yra padaryta, o ne apie valstybės, iš kurios yra daroma žala, atsakomybę. Tikėtis, kad priešiška valstybė atlygintų savo (arba jos leistais) hibridinio karo veiksmais padarytą žalą privatiems subjektams būtų beviltiška.

Kalbant apie valstybės atsakomybę, būtina vertinti jos pačios pareigas užtikrinti aplinką, kad nebūtų daroma žala arba bent jau ji būtų minimalizuojama. Taigi, valstybės atsakomybė už sukeltą žalą galėtų kilti ne tik dėl pačios valstybės kokių nors tiesioginių veiksmų, bet ir dėl neveikimo, t.y. nepakankamo prevencinių priemonių užtikrinimo. Ši idėja nėra jokiais būdais svetima Lietuvos teisiniame reguliavime. Pavyzdžiui, CK 6.271 straipsnyje yra numatyta valstybės atsakomybė už valdžios institucijų neteisėtus veiksmus. Šiame kontekste svarbu paminėti, jog pagal to paties straipsnio 3 dalį valstybės atsakomybė kyla ir už neveikimą. Pareigą užtikrinti tinkamas prevencines priemones galima įžvelgti Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje. Pavyzdžiui, vienoje konstitucinės justicijos byloje teismas yra nurodęs, kad pagal Konstituciją valstybės valdžios ir valdymo institucijos turi pareigą užtikrinti visuomenės saugumą ir viešąją tvarką, saugoti asmenį nuo kėsinosi į jo gyvybę bei sveikatą, ginti žmogaus teises ir laisves¹⁸. Panašios nuostatos laikosi ir Europos Žmogaus Teisių Teismas¹⁹. Taigi, matome, kad valstybės civilinė atsakomybė nėra atmetina.

Manome, kad valstybės civilinė atsakomybė už kibernetinių atakų sukelimą žalą tam tikromis sąlygomis turėtų būti taikoma, nes priešingu atveju kyla grėsmė civilinių teisių santykių stabilumui. Kibernetinių atakų atveju kaltą asmenį būna sunku nustatyti, o net jį nustačius žalos atlyginimas gali būti praktiškai neįmanomas. Laikytina, kad atsakomybės už kibernetines atakas negalima perkelti vien priešiška valstybei ar asmenims (grupuotėms), nes iš Konstitucijos valstybei kyla pareiga rūpintis visuomenės saugumu ir viešąja tvarka.

¹⁸ Lietuvos Respublikos Konstitucinio Teismo 2001 m. balandžio 12 d. nutarimas. *Valstybės žinios*, 30-977.

¹⁹ K.U. prieš Suomiją [EŽTT], Nr. 2872/02, [2008-12-02]. ECLI:CE:ECHR:2008:1202 JUD000287202, 40-43 p., taip pat Önerildiz prieš Turkiją [EŽTT], Nr. 48939/99, [2004-11-30]. ECLI:CE:ECHR:2004:1130 JUD004893999, 71 ir 90 p.

Diversinės atakos (sabotažas)

Skirtingai nuo kitų formų, diversinės atakos (sabotažas) yra kinetinė hibridinio karo priemonė, t. y. jos padariniai dažniausiai pasireiškia tiesiogine fizine žala materialiams objektams. Taigi, kitaip nei dezinformacijos kampanijos ar kibernetiniai išpuoliai, sabotažas veikia ne skaitmeninę ar informacinę erdvę, bet pačią infrastuktūrą – nekilnojamąjį turtą, įrangą, jungtis ir kitus klasikinius civilinės apyvartos objektus. Šiai priemonei būdinga ir tai, kad žala dažniausiai padaroma tiesioginiu asmenų veikimu, todėl sabotažo atvejais neretai galima nustatyti ir atsakomybės patraukti konkretų žalą sukėlusius veiksmus atlikusį subjektą.

Poveikis privataus sektoriaus interesams

Jau minėta, kad sabotažo veiksmai savo esme nukreipti į tai, kad fiziškai būtų sunaikinti arba sugadinti tam tikri infrastruktūros objektai, todėl tokie išpuoliai neišvengiamai daro įtaką nuosavybės teisėms ir jų įgyvendinimui. Istoriškai sabotažo atakos (kariniame kontekste) siejamos su valstybės saugumo pakirtimu, pirmiausia kariniais pajėgumais, tačiau jais toli gražu neapsiribojant. Atsižvelgiant į tai, teisingiausia būtų kritinės valstybės infrastruktūros sąvoka. Šiuo metu dažniausiai minimi kritinės infrastruktūros objektai yra telekomunikacijų ir duomenų perdavimo linijos, povandeniniai kabeliai, energetikos tinklai, dujų ir naftos tiekimo vamzdynai, elektros perdavimo infrastruktūra, geležinkelių ir kelių jungtys, taip pat įvairūs objektai, užtikrinantys kartinį valstybės ekonominį ir socialinį funkcionavimą. Itin reikšminga tai, kad didelė dalis tokios infrastruktūros – nors strategiškai svarbi valstybei – faktiškai priklauso privatiems subjektams arba yra jų eksploatuojama. Ši tendencija matoma net karinės logistikos srityje, kuri tradiciškai laikoma išimtinė valstybės atsakomybe: apie 90 procentų NATO karinių transportų naudojami civiliniu turtu, daugiau nei pusė palydovinio ryšio gynybos poreikiams teikiama komercinio sektoriaus, o 75 procentai priimančiųjų valstybių paramos NATO operacijoms grindžiamos vietinių komercinių subjektų paslaugomis.²⁰ Kitose kritinės infrastruktūros srityse privataus sektoriaus vaidmuo yra dar labiau dominuojantis, todėl bet koks sabotažo veiksmas, formaliai nukreiptas prieš valstybės strateginius pajėgumus, praktiškai pirmiausia pažeidžia būtent privačią nuosavybę.

Lietuvos nacionalinio saugumo doktrinoje aiškiai įtvirtinta, kad nepriklausoma demokratinė valstybė privalo užtikrinti saugų Tautos gyvumą²¹, o tai savaime ap-

²⁰ EDWARDS, Charlie ir SEIDENSTEIN, Nate (2025). *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure* [interaktyvus]. Prieiga per internetą: <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian-sabotage-operations-against-europes-critical-infrastructure/> [žiūrėta 2026 sausio 25 d.].

²¹ Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas. 1996 m. gruodžio 19 d. Nr. VIII-49. *Valstybės žinios*, 1997, 2-16.

ima ir kritinės infrastruktūros apsaugą, kaip vieną iš pagrindinių saugumo prielaidų. Vis dėlto šios pareigos įgyvendinimas tampa gerokai sudėtingesnis, kai esminiai valstybės funkcionavimui būtini infrastruktūros pajėgumai priklauso privatiems subjektams. Kritinės infrastruktūros privatumas reiškia, kad valstybė negali visiškai kontroliuoti su saugumu susijusių rizikų, o sabotažo atveju pirminė fizinė žala tenka būtent savininkams. Be to, privatus sektorius iš savo prigimties orientuojasi į pelno maksimizavimą ir veiklos efektyvumą (akcininkų interesų teorija), todėl natūraliai linkęs investuoti į tas sritis, kurios tiesiogiai generuoja ekonominę grąžą²², o ne į perteklines saugumo priemones. Tokia interesų asimetrija tarp valstybės saugumo poreikių ir privataus sektoriaus prioritetų lemia, kad kritinės infrastruktūros atsparumo užtikrinimas sabotažo grėsmėms tampa bendro valstybinio ir privačiojo sektoriaus sąveikos iššūkiu, kuriame valstybė privalo ieškoti papildomų reguliacinių ir organizacinių sprendimų.

Siekdama sustiprinti kritinės infrastruktūros apsaugą ir suvaldyti sabotažo keliamas rizikas, valstybė 2025 m. gegužės mėn. pakeitė Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymą. Pagal naują įstatymo redakciją nacionaliniam saugumui svarbių įmonių, įrenginių ir turto fizinės apsaugos reikalavimai nustatomi vadovaujantis Viešojo saugumo tarnybos prie Vidaus reikalų ministerijos patvirtintu nacionaliniam saugumui užtikrinti svarbių įmonių ir infrastruktūros fizinės apsaugos standartu.²³ Įgyvendinant šią nuostatą, 2025 m. lapkritį Viešojo saugumo tarnyba patvirtino valstybei svarbių objektų fizinės saugos užtikrinimo standartą, kuriuo siekiama standartizuoti fizinės apsaugos reikalavimus įvairiems nacionaliniam saugumui svarbiems pajėgumams, atsižvelgiant į praktikoje identifikuotas rizikas ir gerąsias saugumo priemones.²⁴ Nors šiais standartais siekiama sustiprinti nacionaliniam saugumui svarbių objektų apsaugą, nėra aišku, kiek ir kokia apimtimi jie gali riboti pačių kritinės infrastruktūros subjektų interesus. Kadangi standarto turinys nėra viešai prieinamas, galima tik daryti prielaidą, kad juo nustatomi papildomi saugumo reikalavimai, galintys keisti įprastas privačių subjektų veiklos praktikas, didinti jų pareigas ir finansinę naštą ar riboti diskreciją sprendžiant dėl infrastruktūros valdymo.

Be to, atsižvelgiant į pastarųjų metų hibridinio karo tendencijas, matyti, kad sabotažo išpuoliai vis dažniau kėsinais ne tik į kritinę infrastruktūrą, bet ir į įprastus

²² DANIELSON, Morris G., HOGAN, Karen M. Ir OLSON, Gerard T. (2024). *Shareholder theory, stakeholder theory, and the capital budgeting decision* [interaktyvus]. Prieiga per internetą: <https://virtusinterpress.org/Shareholder-theory-stakeholder-theory-and-the-capital-budgeting-decision.html> [žiūrėta 2026 sausio 25 d.].

²³ Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo Nr. IX-1132 1, 2, 6, 12, 18 straipsnių pakeitimo įstatymo projektas. 2025. 25-4127(2);

²⁴ Lietuvos Respublikos vidaus reikalų ministerija. Patvirtintas valstybei svarbių objektų fizinės apsaugos standartas [interaktyvus]. Prieiga per internetą: <https://vrm.lrv.lt/lt/naujienos/patvirtintas-valstybei-svarbiu-objektu-fizines-saugos-uztikrinimo-standartas-u2BP/> [žiūrėta 2026 sausio 25 d.].

„civilius“ verslus. Šį procesą iliustruoja ir 2024 m. gegužę Vilniuje kilęs gaisras IKEA prekybos centre, dėl kurio pradėtas tyrimas pagal terorizmo požymius²⁵, kas leidžia manyti, jog kariniai sabotazo veiksmai šiame kontekste gali peraugti į terorizmą ar veikti jam artimu pobūdžiu.

Atsižvelgiant į tai, privataus sektoriaus vaidmuo civilinėje apyvartoje neišvengiamai kinta: saugumas tampa ne papildoma pasirinkimo galimybe, bet būtina veiklos sąlyga. Tai reiškia, kad verslai turi investuoti į rizikos valdymą, infrastruktūros apsaugą ir veiklos tęstinumo priemones taip pat nuosekliai, kaip įprastai investuojama į veiklos plėtrą ar efektyvumą.

Poveikis civilinei atsakomybei

Skirtingai nei kitų hibridinio karo formų atvejais, kur veikėjai dažnai lieka anonimiški, diversantai neretai identifikuojami, sulaikomi ir patraukiami atsakomybėn tiek baudžiamąja, tiek civiline tvarka. Tai lemia tiesioginis ir aiškiai nustatomas jų veiksmų pobūdis, leidžiantis tiksliai atriboti, kas sukėlė žalą ir kokie veiksmai tai nulėmė.

Civilinės teisės požiūriu sabotazo atvejai patenka į bendrosios deliktinės atsakomybės taikymo sritį. CK 6.263 straipsnyje įtvirtinta, kad kiekvienas asmuo privalo laikytis tokio elgesio taisyklių, kad savo veiksmais nepadarytų žalos kitam, o padarytą žalą turi visiškai atlyginti žalą sukėlęs asmuo. Tai reiškia, kad būtent sabotazą įvykdęs subjektas yra pirminis ir tiesioginis civilinės atsakomybės adresatas: jis atsako už žalą, padarytą tiek asmenims, tiek turtui, nepriklausomai nuo hibridinio karo aplinkybių ar kitų išorinių veiksnių. Kadangi sabotazo esmė yra tyčinis fizinis poveikis turtui, tokie atvejai kvalifikuojami kaip akivaizdus CK 6.263 straipsnyje nurodytos pareigos pažeidimas, o atsakomybė kyla būtent pačiam veiksmus atlikusiam asmeniui.

Vis dėlto keičiantis laikams ir modernėjant technologijoms, sabotazo pobūdis taip pat kinta. Fizinis diversanto dalyvavimas ne visada yra būtinas, o destruktiniai veiksmai gali būti atliekami pasitelkiant nuotoliniu būdu valdomas sistemas, ypač dronus. Tokios priemonės leidžia atlikti išpuolius fiziškai neperžengiant valstybių sienų, arba pasirūpinant, jog būtų neįmanoma nustatyti, iš kurios teritorijos jos buvo valdomos. Dėl to tradicinė, aiškiai atribojama sabotazo schema ima artėti prie kibernetinių ar kitų anonimiškumą užtikrinančių hibridinių atakų modelių, kur tikrojo kaltininko identifikavimas bei patraukimas atsakomybėn tampa sudėtingas arba apskritai neįmanomas. Tai puikiai iliustravo 2025 m. rugsėjį fiksuoti dronų antskrydžiai Vakarų

²⁵ LRT Radioteka. Generalinė prokuratūra: IKEA Vilniuje pernai sukeltas gaisras buvo teroro aktas [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/radioteka/irasas/2000398372/generaline-prokuratura-ikea-vilniuje-pernai-sukeltas-gaisras-buvo-teroro-aktas> [žiūrėta 2026 sausio 25 d.].

Europos oro uostuose, kai dėl nuotolinio valdymo pobūdžio teisėsaugai nepavyko nustatyti atsakingų subjektų.²⁶

Kitos hibridinio karo priemonės

Be jau aptartų dezinformacijos kampanijų, kibernetinių atakų ir diversinių veiksmų, hibridinio karo kontekste galima išskirti ir kitas priemones, kurios pasižymi didele įvairove ir dėl savo specifikos negali būti susistemintos ar priskirtos iki tol aptartoms hibridinio karo formoms. Vis dėlto, nepaisant skirtingumo, kitas hibridinio karo priemones vienija bendras poveikis – jos trikdo įprastą civilinių teisinių santykių funkcionavimą ir destabilizuoja civilinę apyvarą, sutarčių vykdymą bei civilinių santykių subjektų teisėtų lūkesčių įgyvendinimą.

Analizuojant kitas hibridinio karo priemones pažymėtina, kad pastaraisiais metais Lietuvoje susiduriama su itin ryškiomis hibridinėmis grėsmėmis, kylančiomis iš Baltarusijos Respublikos. Didžiąja dalimi nukreiptos į transporto ir logistikos sektorius, šios grėsmės reikšmingai paveikė įprastą paslaugų teikimą, krovinių judėjimą. Ryškiausiais to pavyzdžiais galime laikyti Baltarusijos vykdytą Lietuvos vežėjų sulaikymą ir judėjimo ribojimą jos teritorijoje²⁷ bei meteorologinių balionų paleidimus į Lietuvos oro erdvę, kuriais keliama grėsmė skrydžių saugumui ir tuo pačiu trikdoma aviacijos sektoriaus veikla.²⁸

Baltarusijos vykdytas Lietuvos vežėjų sulaikymas ir judėjimo ribojimas jos teritorijoje lėmė reikšmingus transporto paslaugų sutrikdymus, krovinių judėjimo sustojimą bei prastovas. Dėl vilkikų priverstinio stovėjimo buvo patiriami finansiniai nuostoliai, susiję su vėluojančiais pristatymais, sutartinių sankcijų taikymu ir papildomomis veiklos sąnaudomis, todėl dalis vežėjų ėmė reikšti reikalavimus dėl patirtos žalos kompensavimo iš valstybės lėšų.²⁹ Vis dėlto įvertinus nuosekliai priešišką Baltarusijos režimo laikyseną Lietuvos Respublikos atžvilgiu ir viešai žinomą hibridinio karo fakto egzistavimą, pažymėtina, kad vežėjai, vykdydami komercinę veiklą per šios valstybės teritori-

²⁶ Euronews. Fact-checking Europe's drone problem: Why are airports closing over drone sightings? [interaktyvus]. Prieiga per internetą: <https://www.euronews.com/my-europe/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shuttering-over-drone-sightings> [žiūrėta 2026 sausio 25 d.].

²⁷ LRT. Minskas: Baltarusija neleis išvykti Lietuvos vilkikams, kol bus uždaryta siena [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/eismas/7/2742128/minskas-baltarusija-neleis-isvykti-lietuvos-vilkikams-kol-bus-uzdaryta-siena?> [žiūrėta 2026 sausio 25 d.].

²⁸ LRT. Lietuvos oro uostai skaičiuoja žalą dėl balionų: nuostoliai per 750 tūkst. eurų [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/verslas/4/2762356/lietuvos-oro-uostai-skaiciuoja-zala-del-balionu-nuostoliai-per-750-tukst-euru> [žiūrėta 2026 sausio 25 d.].

²⁹ LRT. Taminskas sako, kad vežėjai rizikavo patys, todėl Lietuva patirtų nuostolių nekompensuos [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/eismas/7/2751042/taminskas-sako-kad-vezejai-rizikavo-patys-todel-lietuva-patirtu-nuostoliu-nekompensuos> [žiūrėta 2026 sausio 25 d.].

ją, turėjo realią galimybę ir pareigą numatyti galimas geopolitines rizikas bei tikėtinus veiklos sutrikdymus. Kaip jau minėta, šiuolaikinių hibridinių grėsmių sąlygomis privatus subjektai privalo bendradarbiauti su valstybės institucijomis ir patys aktyviai rūpintis savo veiklos saugumu bei prisiimti su tuo susijusią atsakomybę. Be to, nagrinėjamoje situacijoje nėra pagrindo konstatuoti Lietuvos valdžios institucijų neteisėtų veiksmų ar neveikimo, kaip tai suprantama pagal CK 6.271 straipsnio 1 dalį. Lietuvos pasienio punktų uždarymas buvo taikomas kaip saugumo užtikrinimo priemonė, o faktinius vežėjų judėjimo ribojimus vykdė Baltarusijos režimas. Atsižvelgiant į tai, vežėjų reikalavimai atlyginti patirtus nuostolius iš valstybės biudžeto laikytini iš esmės nepagrįstais. Analogiškos pozicijos laikosi ir Lietuvos Respublikos vyriausybė.³⁰

Antruoju atveju, meteorologinių balionų situacija pasižymi trimis esminiais aspektais, kurie leidžia ją vertinti kitaip nei vežėjų sulaikymą. Pirma, oro uostai, oro bendrovės ir keleiviai savo veiklą vykdė Lietuvos Respublikos teritorijoje ir savo veiksmais niekaip nepasirinko palaikyti kontakto su priešiško režimo valstybe. Dėl šios priežasties jiems negali būti perkeliama rizika, kylanti iš priešiškos valstybės vykdomų hibridinių veiksmų. Antra, meteorologinių balionų pasitelkimas kontrabandai buvo žinomas gerokai anksčiau, nei jie pradėti sistemingai naudoti aviacijos veiklos trikdymui³¹, todėl tokio pobūdžio grėsmė galėjo būti numatyta valstybės institucijų lygmeniu kaip tikėtina hibridinio karo priemonė. Trečia, tokių grėsmių neutralizavimas negali būti užtikrintas privačių subjektų pastangomis, nes saugumo ir oro erdvės apsaugos užtikrinimas yra valstybės funkcija. Be to, tikėtina, kad meteorologinių balionų pašalinimas gali reikalauti kovinių ginklų panaudojimo, kuris pagal Lietuvos Respublikos kovinių ginklų naudojimo krašto apsaugos sistemoje statuto patvirtinimo įstatymą priskirtas išimtinai valstybės institucijų ir kariuomenės kompetencijai. Atsižvelgiant į visas šias aplinkybes, darytina išvada, kad egzistuoja tam tikras pagrindas kalbėti apie galimą valstybės institucijų neveikimą ar nepakankamą reagavimą į žinomą ir prognozuojamą grėsmę, o tai savo ruožtu gali lemti žalos atlyginimo pareigą pagal CK 6.271 straipsnį.

Neatsitiktinai Lietuvos Respublikos 2026–2028 metų biudžeto patvirtinimo įstatyme (13 straipsnio 6 dalis) Lietuvos Respublikos susisiekimo ministerijai suteikta teisė iš savo asignavimų skirti lėšų priemonėms, skirtoms reaguoti į kaimyninių valstybių priešiškas Lietuvai hibridines atakas ir kitus neteisėtus veiksmus, taip pat šių veiksmų padariniams šalinti bei dėl jų patirtiems finansiniams nuostoliams ūkio subjektams kompensuoti. Valstybės biudžete numatytos lėšos patvirtina, kad hibridinės atakos vertinamos ne tik kaip saugumo problema, bet ir kaip reiškinys, turintis realią pasekmių civiliniams teisiniams santykiams. Taip pat įstatymų leidėjas šiuo reguliavimu

³⁰ Ibid.

³¹ LRT. Minsko balionų istorija: kada jie pradėjo skristi į Lietuvą ir ko ėmėmės [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/verslas/4/2770271/minsko-balionu-istorija-kada-jie-pradejo-skristi-i-lietuva-ir-ko-ememes?> [žiūrėta 2026 sausio 25 d.].

parodo valstybės siekį aktyviai įsitraukti į hibridinio karo sukeltų pasekmių šalinimą ir prisidėti prie civilinės apyvartos stabilumo atkūrimo.

Manytina, kad pagal tokią valstybės pasirinktą poziciją būtų tikslinga formuoti specialų fondą, skirtą hibridinio karo veiksmų sukeltiems nuostoliams kompensuoti ne tik transporto sektoriuje, bet ir platesniame kontekste. Atitinkamas mechanizmas galėtų būti taikomas įvairių hibridinių atakų atvejais sukeltai fizinei žalai atlyginti, kai žalos padarę subjektai nėra nustatomi arba realiai neįmanoma iš jų išsieškoti nuostolių. Centralizuotas kompensavimo sprendimas padėtų užtikrinti didesnę civilinių teisių santykių stabilumą ir teisingesnę rizikos paskirstymą tarp valstybės ir privačių subjektų hibridinių grėsmių sąlygomis.

Išvados

Hibridinis karas turėtų būti suvokiamas kaip įvairių (kombinuotų) kinetinių ir nekinetinių priemonių naudojimas nepereinant į karo stadiją konvencine (tradicine) prasme.

Išskirtinos keturios aktualios hibridinio karo priemonių grupės: dezinformacijos kampanijos, kibernetinės atakos, diversinės atakos ir kitos priemonės.

Dezinformacijos kampanijos gali paveikti civilinius teisinius santykius, susijusius su asmens garbe ir orumu, taip pat dalykine reputacija. Skleidžiant tikrovės neatitinkančią informaciją gali daugėti CK 2.24 straipsnyje numatytų pažeidimų, o reputacijos bloginimas gali apsunkinti sandorių sudarymą.

Kibernetinės atakos kelia reikšmingų iššūkių deliktinei civilinei atsakomybei, nes apsunkina žalą sukėlusio subjekto nustatymą ir realų žalos atlyginimą. Dėl šios priežasties svarstyta valstybės civilinė atsakomybė už neveikimą kibernetinio saugumo srityje.

Sabotažas pirmiausia pažeidžia privačią kritinę infrastruktūrą ir kitus civilinius objektus, todėl didėja tiek valstybės reguliavimo, tiek privačių subjektų atsakomybė už saugumo užtikrinimą. Civilinės atsakomybės požiūriu dažniausiai taikoma bendroji deliktinė atsakomybė.

Kitų hibridinio karo priemonių sukeltos žalos atlyginimas, ypač transporto ir logistikos sektoriuose, gali lemti tiek ūkio subjektų, tiek valstybės atsakomybę, todėl tikslinga svarstyti specialaus kompensavimo fondo steigimą.

Šaltinių sąrašas:

Teisės norminiai aktai

Lietuvos Respublikos civilinis kodeksas. 2000 m. liepos 18 d. Nr. VIII-1864. Valstybės žinios, 2000, 74-2262;

Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas. 1996 m. gruodžio 19 d. Nr. VIII-49. Valstybės žinios, 1997, 2-16;

Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo Nr. IX-1132 1, 2, 6, 12, 18 straipsnių pakeitimo įstatymo projektas. 2025. 25-4127(2); Lietuvos Respublikos 2026-2028 metų biudžeto patvirtinimo įstatymas. 2025 m. gruodžio 11 d. Nr. XV-651. TAR, 2025-12-22, Nr. 22321.

Specialioji literatūra

HOFFMAN G., Frank (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies;

MUMFORD, Andrew ir CARLUCCI, Pascal (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, 8(2),192-206;

BARGAOANU, Alina ir NEGREA-BUSUIOC, Elena (2024). Hybrid Warfare is Less Than Warfare: A Dangerous Illusion [interaktyvus]. Prieiga per internetą: https://irregular-warfarecenter.org/wpcontent/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf [žiūrėta 2026 sausio 25 d.].

FRIDMAN, Ofer (2018). Russian 'Hybrid Warfare'. Resurgence and Politicisation. New York: Oxford University Press;

BYMAN, Daniel (2025). Foreign Malign Influence Targeting U.S. and Allied Corporations [interaktyvus]. Prieiga per internetą: <https://www.csis.org/analysis/foreign-malign-influence-targeting-us-and-allied-corporations> [žiūrėta 2026 sausio 25 d.].

SCHULZKE, Marcus. (2018). The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. *Perspectives on Politics*, 16(4), 954–968;

EDWARDS, Charlie ir SEIDENSTEIN, Nate (2025). The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure [interaktyvus]. Prieiga per internetą: <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/> [žiūrėta 2026 sausio 25 d.].

DANIELSON, Morris G., HOGAN, Karen M. Ir OLSON, Gerard T. (2024). Shareholder theory, stakeholder theory, and the capital budgeting decision [interaktyvus]. Prieiga per internetą: <https://virtusinterpress.org/Shareholder-theory-stakeholder-theory-and-the-capital-budgeting-decision.html> [žiūrėta 2026 sausio 25 d.].

Teismų praktika

Lietuvos Aukščiausiojo Teismo 2025 m. vasario 27 d. nutartis civilinėje byloje Nr. e3K-7-4-403/2025;

Lietuvos Respublikos Konstitucinio Teismo 2001 m. balandžio 12 d. nutarimas. Valstybės žinios, 30-977;

K.U. prieš Suomiją [EŽTT], Nr. 2872/02, [2008-12-02]. ECLI:CE:ECHR:2008:1202 JUD000287202;

Öneryıldız prieš Turkiją [EŽTT], Nr. 48939/99, [2004-11-30]. ECLI:CE:ECHR:2004:1130 JUD004893999.

Kiti šaltiniai

GOTEV, Georgi (2021-10-28). The Brief, powered by Facebook – Hybrid warfare [interaktyvus]. Prieiga per internetą: <https://www.euractiv.com/opinion/the-brief-powered-by-facebook-hybrid-warfare/> [žiūrėta 2026 sausio 25 d.].

- European Union External Action (2025-03-14) Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI) [interaktyvus]. Prieiga per internetą: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#45330 [žiūrėta 2026 sausio 25 d.].
- Kiel Institut (2025-10) Ukraine Support Tracker Data [interaktyvus]. Prieiga per internetą: <https://www.kielinstitut.de/publications/ukraine-support-tracker-data-6453/> [žiūrėta 2026 sausio 25 d.].
- The Guardian. Russian cyber-attacks against NATO states up by 25% in a year, analysis finds [interaktyvus]. Prieiga per internetą: <https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds> [žiūrėta 2026 sausio 25 d.].
- Atlantic Council (2024-02-29). Undermining Ukraine: How Russia widened its global information war in 2023 [interaktyvus]. Prieiga per internetą: <https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/> [žiūrėta 2026 sausio 25 d.].
- LRT. Janutienė viešai paneigė apie „Laisvės TV“ ir Tapiną išsakytus žodžius [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/lietuvoje/2/2705463/janutiene-viesai-paneige-apie-laisves-tv-ir-tapina-issakytus-zodzius> [žiūrėta 2026 sausio 25 d.].
- Wall Street Journal. Russian Intelligence Is Pushing False Claims of U.S. Biological Testing in Africa, U.S. Says [interaktyvus]. Prieiga per internetą: <https://www.wsj.com/world/africa/russian-intelligence-is-pushing-false-claims-of-u-s-biological-testing-in-africa-u-s-says-ea817592> [žiūrėta 2026 sausio 25 d.].
- Lietuvos Respublikos vidaus reikalų ministerija. Patvirtintas valstybei svarbių objektų fizinės apsaugos standartas [interaktyvus]. Prieiga per internetą: <https://vrm.lrv.lt/lt/naujienos/patvirtintas-valstybei-svarbiu-objektu-fizines-saugos-uztikrinimo-standartas-u2BP/> [žiūrėta 2026 sausio 25 d.].
- LRT Radioteka. Generalinė prokuratūra: IKEA Vilniuje pernai sukeltas gaisras buvo teroro aktas [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/radioteka/irasas/2000398372/generaline-prokuratura-ikea-vilniuje-pernai-sukeltas-gaisras-buvo-teroro-aktas> [žiūrėta 2026 sausio 25 d.].
- Euronews. Fact-checking Europe's 'drone problem': Why are airports closing over drone sightings? [interaktyvus]. Prieiga per internetą: <https://www.euronews.com/my-europe/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shutting-over-drone-sightings> [žiūrėta 2026 sausio 25 d.].
- LRT. Minskas: Baltarusija neleis išvykti Lietuvos vilkikams, kol bus uždaryta siena [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/eismas/7/2742128/minskas-baltarusija-neleis-isykti-lietuvos-vilkikams-kol-bus-uzdaryta-siena> [žiūrėta 2026 sausio 25 d.].
- LRT. Lietuvos oro uostai skaičiuoja žalą dėl balionų: nuostoliai per 750 tūkst. eurų [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/verslas/4/2762356/lietuvos-oro-uostai-skaiciuoja-zala-del-balionu-nuostoliai-per-750-tukst-euru> [žiūrėta 2026 sausio 25 d.].

LRT. Taminskas sako, kad vežėjai rizikavo patys, todėl Lietuva patirtų nuostolių ne-kompensuos [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/eis-mas/7/2751042/taminskas-sako-kad-vezejai-rizikavo-patys-todel-lietuva-patirtu-nuos-toliu-nekompensuos> [žiūrėta 2026 sausio 25 d.].

LRT. Minsko balionų istorija: kada jie pradėjo skristi į Lietuvą ir ko ėmėmės [interaktyvus]. Prieiga per internetą: <https://www.lrt.lt/naujienos/verslas/4/2770271/minsko-balio-nu-istorija-kada-jie-pradejo-skristi-i-lietuva-ir-ko-ememes?> [žiūrėta 2026 sausio 25 d.].