MYKOLO ROMERIO UNIVERSITETO
VIEŠOJO SAUGUMO AKADEMIJA

KASPARAS STONKUS
TEISĖ IR POLICIJOS VEIKLA (SPECIALIZACIJA: IKITEISMINIS PROCESAS)

HIBRIDINĖS GRĖSMĖS KAIP IŠŠŪKIS LIETUVOS NACIONALINIAM SAUGUMUI

Magistro baigiamasis darbas

Vadovas: Doc. dr. Eglė Štareikė

Kaunas, 2026

TURINYS

SANTRUMPŲ SĄRAŠAS

NATO – Šiaurės Atlanto Sutarties Organizacija;

ES – Europos Sąjunga;

LR – Lietuvos Respublika;

BK – Baudžiamasis kodeksas;

NKVC – Nacionalinis krizių valdymo centras;

NKSC – Nacionalinis kibernetinio saugumo centras;

NKC – Nacionalinis koordinavimo centras;

VRM – Vidaus reikalų ministerija.

ĮVADAS

Temos aktualumas ir naujumas. Šiandieninėje, ypatingai įtemptoje geopolitinėje situacijoje, hibridinės grėsmės yra vienas iš sudėtingiausių ir greičiausiai besikeičiančių reiškinių tiek Lietuvoje, tiek ir Europoje. Karas Ukrainoje, migrantų krizė, meteorologiniai balionai, dronai ir kitos hibridinio pobūdžio atakos tapo didžiuliu iššūkiu Lietuvos nacionaliniam saugumui. Hibridinės grėsmės atskleidė, jog vien tik stipri valstybės karinė galia, nebegarantuoja apsaugos nuo netradicinių ir daugialypių priemonių panaudojimo, siekiant paveikti gyventojų saugumo jausmą, pasitikėjimą valstybinėmis institucijomis ir valstybės stabilumą. Įvertinus tai, valstybės yra priverstos reaguoti į kasdien kylančius naujus iššūkius, keisti ir adaptuoti teisinį reglamentavimą, naudojamas apsaugos priemones, didinti gyventojų sąmoningumą ir stiprinti tarptautinį bendradarbiavimą.

Hibridinių grėsmių tema yra plačiai nagrinėjama užsienio autorių. Hibridinių grėsmių terminas yra pakankamai naujas ir pirmą kartą buvo paminėtas 2007 metais autoriaus Frank G. Hoffman.[1] Kiek vėliau, mokslininkas Sascha-Dominik Bachmann aptarė hibridinių grėsmių turinį, aprašė NATO požiūrį ir pateikė galimus atsakymus į tokio pobūdžio hibridines veiklas.[2] Hibridinio karo sąvokos atsiradimo pradžią ir aplinkybes aprašė Bettina Renz.[3] Europos Sąjungos galimus atsakus į kylančias hibridines grėsmes pateikė Ionut Alin Cirdei, Lucian Ispas.[4] Mikael Weissmann tyrinėjo hibridinio karo ir hibridinių grėsmių supratimą taikos, konflikto ir karo kontekstuose ir kaip šios sąvokos keičia įprastą konfliktų dinamikos supratimą.[5] Georgios Giannopoulos, Hanna Smith ir Marianthi Theocharidou pateikė hibridinių grėsmių konceptualinį modelį, naudojamus įrankius, akcentuodami Europos Sąjungos ir NATO bendradarbiavimą.[6] Hibridinio karo problemas tarptautinėje teisėje nagrinėjo Alaa Al Dakour Al Aridi,[7] o Laura Lisboa išnagrinėjo

[1] Frank G. Hoffman, *Conflict in the 21st century: the rise of hybrid wars,* (Potomac Institute for Policy Studies, 2007), https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
[2] Sascha-Dominik Bachmann, „Hybrid threats, cyber warfare and NATO comprehensive approach for countering 21 st. Century threats – mapping the new frontier of global riskand the security management“, Amicus Curiae 88, 2012, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989808.
[3] Bettina Renz, „Russia and 'hybrid warfare'", Contemporary Politics 22, 3 (2016), https://doi.org/10.1080/13569775.2016.1201316.
[4] Ionut Alin Cirdei, Lucian Ispas, „A possible answer of the European Union to hybrid threats", *Buletin stiintific*, 2, 44, 2017, https://www.armyacademy.ro/buletin/bul2_2017/CARDEI.pdf.
[5] Mikael Weissmann „Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework", Journal on Baltic Security, 5, 1 (2019), https://www.researchgate.net/publication/334967002_Hybrid_warfare_and_hybrid_threats_today_and_tomorrow_towards_an_analytical_framework.
[6] Georgios Giannopoulos, Hanna Smith ir Marianthi Theocharidou, „The landscape of Hybrid Threats: A conceptual model", *European Union and Hybrid CoE*, 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.
[7] Alaa AI Dakour AI Aridi, „Hibridinio karo problema tarpautinėje teisėje" (daktaro disertacija, Vilniaus universitetas, 2022), https://epublications.vu.lt/object/elaba:149038012.

Europos Sąjungos kolektyvinį atsaką į hibridines grėsmes.[8] Nacionalinio saugumo apibrėžimą pateikė užsienio autorius Mitchell Alan Kaplan[9], o Ambrues Monboe Nebo pateikė nacionalinio saugumo sektorių sąrašą.[10]

Akademiniame pasaulyje hibridinių grėsmių tema taip pat aktyviai tiriama ir Lietuvoje. Apie hibridinių grėsmių turinio keliamus iššūkius ir priemones joms įveikti rašė Lietuvos autoriai Eitvydas Bajorūnas ir Vytautas Keršanskas.[11] Atsako į hibridines grėsmes, jų koncepciją, politiką ir strateginį požiūrį tyrė mokslininkės Danguolė Seniutienė ir Laima Paulauskytė[12], o problematinius aspektus kovoje su hibridinėmis grėsmėmis Europos regione išskyrė Eglė Štareikė.[13] Hibridinės grėsmės yra neatsiejamos nuo šalies nacionalinio saugumo. Nacionalinio saugumo poreikio būtinybę ir jo įtaką visuomenės saugumui analizavo Saulius Greičius ir Birutė Pranevičienė.[14] Nacionalinio saugumo politikos ir pilietinės visuomenės sąveikos analizė, saugumo samprata buvo pateikta Rolandos Kazlauskaitės-Markelienės, Audronės Petrauskaitės[15], taip pat ir Vytauto Isodos darbuose.[16] Ieva Karpavičiūtė[17], Mantas Bileišis, Svajūnė Ungurytė-Ragauskienė savo moksliniuose darbuose aptarė Lietuvos nacionaliniam saugumui keliančių hibridinių grėsmių suvokimą, teisinio reguliavimo dinamiką, pasikeitimus ir iššūkius Lietuvoje.[18] Naujausioje Generolo Jono Žemaičio Lietuvos karo akademijos monografijoje, Irmina Matonytė,

---

[8] Laura Lisboa, „How to Protect the EU against Hybrid Threats“, *Policy Brief,* žiūrėta 2023 liepos 9 d., https://youngthinkers.ceps.eu/how-to-protect-the-eu-against-hybrid-threats/.

[9] Mitchell Alan Kaplan, „The Socioeconomic and Political Ramifications of Climate Migration in the 21st Century”, (IGI Global Scientific Publishing, 2024), https://www.researchgate.net/publication/359882823_The_Socioeconomic_and_Political_Ramifications_of_Climate_Migration_in_the_21st_Century.

[10] Ambrues Monboe Nebo, „National Security Strategy: A Toolkit for Assessing State Preparedness to Combat Global Security Threats That Endanger National Security in the 21st Century”, *ISRG Journal of Arts Humanities & Social Sciences* 2, 5 (2024), https://doi.org/10.5281/zenodo.13953887.

[11] Eitvydas Bajarūnas, Vytautas Keršanskas, „Hibridinės grėsmės: turinio, keliamų iššūkių ir priemonių įveikti jas analizė”, Lietuvos metinė strateginė apžvalga, 16, 2017-2018, https://kam.lt/wp-content/uploads/2023/01/Bajarunas-Kersanskas.-Hibridines-gresmes-turinio-keliamu-issukiu-ir-priemoniu-iveikti-jas-analize.-Metine-strategine-apzvalga-LKA-2017-2018.pdf.

[12] Danguolė Seniutienė, Laima Paulauskytė, „Response to Hybrid Threats: Policies, Concepts and Strategic Approaches“, *Public Security and Public Orde*r 36 (2024), https://doi.org/10.13165/PSPO-24-36-14.

[13] Eglė Štareikė, „Countering Hybrid Threats: Problematic Aspects in the European Region”, Public Security and Public Order, 36, (2024): 229, https://doi.org/10.13165/PSPO-24-36-17.

[14] Saulius Greičius, Birutė Pranevičienė, „Asmens ir valstybės saugumo samprata, užtikrinimo poreikis ir problemos”, *Regnum est: 1990 m. Kovo 11-osios nepriklausomybės Aktui-20: Liber Amicorum Vytautui Landsbergiui,* 2010, https://cris.mruni.eu/server/api/core/bitstreams/838726e2-7251-4e09-b912-35402bb5652b/content.

[15] Rolanda Kazlauskaitė-Markelienė, Audronė Petrauskaitė, „Pilietinė visuomenė ir nacionalinis saugumas: teorine problemos apžvalga”, *Generolo Jono Žemaičio Lietuvos karo akademija* 9, 1 (2011), https://doi.org/10.47459/lmsa.2011.9.11.

[16] Vytautas Isoda, „Visuomenės ontologinio saugumo samprata: Lietuvos nacionalinio saugumo ontologinė dimensija”, *Visuomenės saugumas ir viešoji tvarka* 18 (2017), https://ojs.mruni.eu/ojs/vsvt/article/view/5618/4825.

[17] Ieva Karpavičiūtė, „Securitization and Lithuania’s National Security Change”, *Lithuanian Foreign Policy Review* 36 (2017), https://doi.org/10.1515/lfpr-2017-0005.

[18] Mantas Bileišis, Svajūnė Ungurytė-Ragauskienė, „Nacionalinio saugumo iššūkiai: viešojo valdymo tobulinimo aktualijos“, iš *Saugumo iššūkiai: Vadybos tobulinimas: Kolektyvinė monografija* (Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2020), https://vb.lka.lt/object/elaba:89853199/89853199.pdf.

Ieva Gajauskaitė ir Viktor Denisenko atskleidė Lietuvos institucijų ir visuomenės supratimą apie hibridines grėsmes.[19]

Darbo problema. Baigiamajame darbe mokslinė problema formuluojama klausimu: kokie yra pagrindiniai hibridinių grėsmių (meteorologinių balionų incidentų ir kibernetinių išpuolių) keliami iššūkiai Lietuvos nacionaliniam saugumui?

Tikslas. Išanalizuoti pasirinktas hibridines grėsmes (meteorologinių balionų incidentus ir kibernetinius išpuolius) kaip kompleksinį iššūkį Lietuvos nacionaliniam saugumui.

Tyrimo uždaviniai.

1. Išanalizuoti hibridinių grėsmių sampratą ir raidą teoriniu aspektu;
2. Išanalizuoti nacionalinio saugumo sampratą hibridinių grėsmių kontekste;
3. Išnagrinėti Europos Sąjungos, NATO strategijas ir partnerystę, hibridinių grėsmių kontekste;
4. Išanalizuoti Lietuvos nacionalinio saugumo strategiją ir priemones, kovojant su hibridinėmis grėsmėmis;
5. Identifikuoti meteorologinių balionų ir kibernetinių išpuolių keliamus iššūkius Lietuvos nacionaliniam saugumui ir teisinio reglamentavimo pasikeitimus.

Ginamasis teiginys. Meteorologinių balionų incidentai ir kibernetiniai išpuoliai veikia „pilkojoje zonoje“, sukeldami teisinio bei institucinio atsako neapibrėžtumą, kuris riboja tradicinių Lietuvos nacionalinio saugumo priemonių efektyvumą taikos metu.

Tyrimo metodika. Nagrinėjant pasirinktą baigiamojo darbo temą, buvo analizuojama Lietuvos ir užsienio autorių mokslinė literatūra, valstybinių institucijų dokumentai. *„Analizė - mokslinio tyrimo metodas, praktiškai ar mintyse suskaidant daiktą, reiškinį, visumą į sudėtines dalis, požymius, savybes, kurios nors dalies, kuri vėliau nagrinėjama atskirai, išskyrimas iš visumos.“*[20] Pasitelkiant lyginamosios analizės metodą, buvo lyginamos skirtingų autorių moksliniuose straipsniuose pateikiamos hibridinių grėsmių, nacionalinio saugumo sampratos. Teisinių dokumentų analizės metodas buvo taikomas analizuojant teisinio reguliavimo pasikeitimus dėl hibridinių grėsmių. Atvejo analizės metodas naudotas nagrinėjant meteorologinių balionų ir kibernetinių išpuolių atvejus Lietuvoje. Taikant aprašomąjį metodą buvo

[19] Irmina Matonytė, Ieva Gajauskaitė ir Viktor Denisenko, *Hibridinės grėsmės: nuo neapibrėžtumo iki atsparumo* (Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2025), https://portalcris.vdu.lt/server/api/core/bitstreams/fe7ffc81-242f-468c-ad96-d175e681ae2e/content.
[20] Rimantas Tidikis, *Socialinių mokslų tyrimų metodologija*, (Vilnius: Lietuvos teisės universitetas, 2003), 375.

interpretuojami moksliniai šaltiniai, ES ir NATO, kitų institucijų dokumentai, strategijos ir teisės aktų analizės rezultatai. Apibendrinimo metodas buvo naudojamas formuluojant ir pateikiant išvadas. *„Apibendrinimas - mąstymo operacija ir produktas, tikrovės reiškinių bendrųjų, esminių požymių ir savybių atspindėjimas.“*[21]

Tyrimo struktūra. Baigiamasis darbas sudarytas iš: įvado, trijų skyrių, išvadų, literatūros sąrašo, santraukos lietuvių ir anglų kalbomis.

Pirmajame baigiamojo darbo skyriuje pristatomas hibridinių grėsmių atsiradimas, pateikiamas jų apibrėžimas, rūšys, atskleidžiamas sąvokos daugialypiškumas. Šioje dalyje taip pat aptariama nacionalinio saugumo sąvoka, jos raida, teoriniai aspektai, pristatomi pagrindiniai saugumo sektoriai, „pilkoji zona”, analizuojama hibridinių grėsmių ir nacionalinio saugumo koreliacija.

Antrajame darbo skyriuje nagrinėjami tarptautiniai Europos Sąjungos, NATO komunikatai, dokumentai, strategijos kovojant su hibridinėmis grėsmėmis ir teisės aktai, atskleidžiamas organizacijų bendradarbiavimo būtinumas. Analizuojami Lietuvos nacionaliniai teisės aktai reglamentuojantys nacionalinį saugumą sąsajoje su hibridinėmis grėsmėmis.

Trečiajame skyriuje, analizuojami meteorologinių balionų ir kibernetinių išpuolių atvejai, atskleidžiama jų, kaip hibridinių grėsmių įtaką Lietuvos nacionaliniam saugumui, pristatomi teisinio reguliavimo pokyčiai, naujų priemonių atsiradimas ir įgyvendinimas.

Darbo pabaigoje pateikiamos išvados.

[21] *Ibid*, 387.

1. HIBRIDINIŲ GRĖSMIŲ IR NACIONALINIO SAUGUMO SAMPRATA, TURINYS IR RAIDA

1.1 Hibridinių grėsmių samprata

Lietuvių kalbos žodyne, žodis „hibridinis" apibrėžiamas kaip „mišrus, gautas kryžminant, susidedantis iš skirtingų dalių.".[22] Šis terminas tiksliai apibūdina, ypatingai šių dienų pasauliniame kontekste - tiek nacionaliniame, tiek ir tarptautiniame lygmenyse vyraujančią opią problemą - hibridines grėsmes. Hibridinės grėsmės pasižymi prigimtiniu bruožu – tradicinių dichtomijų išnykimu ir dviprasmybių kūrimu. Žmonėms iš prigimties būdinga mąstyti ir skirstyti dalykus į dvi griežtai nesuderinamas, priešingas dalis, kaip pavyzdžiui draugas arba priešas, tiesa arba melas. Tačiau, dviprasmybės trukdo tinkamų sprendimų priėmimui, tiek individualiu, tiek ir kolektyviniu lygmeniu, kadangi tai kelia sumaištį ir nepasitikėjimą, todėl tinkamai pasiruošti ir atsakyti į kylančias hibridines grėsmes yra labai problematiška.[23] Hibridinės grėsmės nuolat kinta, evoliucionuoja, todėl atsakas į jas taip pat turi neatsilikti ir pastoviai tobulėti.[24]

Hibridinių grėsmių terminas pirmą kartą buvo paminėtas 2007 metais, amerikiečių karininko, dažnai vadinamo hibridinio karo koncepcijos tėvu, Frank Hoffman. Autoriaus teigimu, hibridinės grėsmės apima visą spektrą skirtingų karo būdų, įskaitant konvencines galimybes, neįprastas taktikas, teroristinius veiksmus, smurtą ir prievartą.[25] Hibridinio tipo veiksmai yra sudėtingi, skirti grasinti, bauginti, destabilizuoti ir sunaikinti taikinį arba sutrikdyti veiklą, taip pat stengtis išlaikyti priešininką ekonominio, politinio karinio ir socialinio disbalanso būsenoje. Dažniausiai subjektas nesuvokia, jog yra užpultas, o nustatyti užpuolimo šaltinį ir tikrųjų ketinimų nėra lengva, todėl kyla problema dėl atsakomųjų veiksmų ir priemonių.[26]

Kolektyvinei gynybai skirtoje, Šiaurės Atlanto Sutarties Organizacijoje - NATO, hibridinių grėsmių terminas oficialiai paminėtas 2010 m. parengtoje NATO strateginėje koncepcijoje. Koncepcijoje, hibridinės grėsmės buvo identifikuotos kaip mažo intensyvumo, kinetinės ir nekinetinės grėsmės tarptautinei taikai ir saugumui, įskaitant tarptautinį terorizmą, piratavimą, išteklių saugumą, tarptautinį organizuotą nusikalstamumą ir demografinius iššūkius.[27]

Hibridinių grėsmių sąvoka pasauliniame kontekste tapo ypač aktuali, po Rusijos įvykdyto Krymo pusiasalio okupacijos. 2014 metais Ukrainoje prasidėjusio konflikto metu, Rusijos Federacijos karinės pajėgos be identifikacinių ženklų įžengė į Krymo pusiasalį ir perėmė jo

---

[22] Lietuvių kalbos žodynas, „Hibridinis reikšmė", žiūrėta 2025 m. lapkričio 15 d., https://www.lietuviuzodynas.lt/terminai/Hibridinis.
[23] Giannopoulos, Hanna Smith ir Marianthi Theocharidou, *supra note,* 6: 6.
[24] Eitvydas Bajarūnas, *„Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond",* European View 19, 1 (2020): 62, https://doi.org/10.1177/1781685820912041.
[25] Hoffman, supra note, 1:8.
[26] *Ibid.*
[27] Bachmann, *supra note*, 2:17.

kontrolę, pradedant administraciniais savivaldos pastatais, automobilių keliais, baigiant oro uostais ir kitais strategiškai svarbiais objektais.[28] Visų įvardintų priemonių visuma, daugumos ekspertų buvo pavadinta puikiu hibridinio karo pavyzdžiu.[29] Iš pradžių, šis terminas susilaukė kritikos dėl aiškaus apibrėžimo nebuvimo ir polinkio jį naudoti kaip viską apimančią sąvoką, tačiau tai sudarė palankias sąlygas diskusijoms apie karybos ateitį ir patį karą, saugumo ir gynybos iššūkius, į kuriuos Vakarų Europos valstybės neturėjo pakankamo atsako.[30]

Mokslininko Mikael Weissmann požiūriu, hibridinis karas ir hibridinės grėsmės yra du to paties reiškinio skirtingi požiūriai arba fazės. Hibridinis karas apima aktyvius veiksmus, taikomus kito subjekto, dažniausiai valstybės, atžvilgiu. Hibridinės grėsmės išsiskiria pasyvumu – jos yra realios arba numanomos, ir kyla iš galimų veiksmų prieš subjektą ateityje.[31]

Europos Komisijos parengtame komunikate, hibridinės grėsmės suprantamos kaip *„prievartinės ir ardomosios veiklos, įprastų ir neįprastų diplomatinių, karinių, ekonominių, technologinių metodų derinys, kuriuo valstybė arba nevalstybiniai subjektai gali siekti konkrečių tikslų oficialiai nepaskelbdami karo. Paprastai siekiama kuo geriau išnaudoti pasirinkto objekto pažeidžiamumą ir sukurti neaiškumą, siekiant apsunkinti sprendimų priėmimo procesus.”*[32]

Europos Vadovų Tarybos tinklapyje hibridinių grėsmių reikšmė pateikiama, kaip *„koordinuota žalinga veikla, kuri planuojama ir vykdoma piktavališkais tikslais. Tokia veikla vykdoma naudojantis įvairiomis priemonėmis, dažnai jas derinant, ir ja siekiama pakenkti taikiniui, pavyzdžiui, valstybei ar institucijai. Šios priemonės gali apimti manipuliavimą informacija, kibernetinius išpuolius, ekonominę įtaką ar prievartą, slaptus politinio manipuliavimo veiksmus, prievartinę diplomatiją arba grasinimus panaudoti karinę jėgą.”*[33]

Hibridinio karo apibrėžimą apsunkina pastovus jo elementų ir priemonių kitimas. Keičiasi tiek istorinės, geografinės ir demografinės sąlygos, tiek ir naudojami ginklai, dalyvaujantys veikėjai ir naudojamos technologijos.[34]

D. Seniutienės ir L. Paulauskytės nuomone, hibridinių grėsmių apibrėžimai gali skirtis, tačiau jie turi išlikti pakankamai lankstūs, kad gebėtų prisitaikyti ir atliepti kintančią jų prigimtį. Vis dėl to sutinkama, kad sąvoka apima prievartinės ir ardomosios veiklos, konvencinių ir

---

[28] James Summers, „The Crimea Crisis: A Case of Occupation, Annexation, Secession or Autonomy?“, Lancaster university law school, žiūrėta 2025 m. lapkričio 8 d., https://lancslaw.wordpress.com/2014/03/05/the-crimea-crisis/.
[29] Andras Racz, „Russia‘s Hybrid War in Ukraine: breaking the enemy‘s ability to resist“ (The Finnish institute of international affairs, 2015), 11, https://fiia.fi/en/publication/russias-hybrid-war-in-ukraine.
[30] Renz, *supra note*, 3: 283.
[31] Weissmann, supra note, 5: 2.
[32] Europos Komisija, „Bendras komunikatas Europos Parlamentui ir Tarybai. Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas“, žiūrėta 2025 m. lapkričio 15 d., http://eur-lex.europa.eu/ legal-content/LT/TXT/?uri=CELEX%3A52016JC0018.
[33] Europos Vadovų Taryba, *„Hibridinės grėsmės”,* žiūrėta 2026 m. sausio 23 d., https://www.consilium.europa.eu/lt/policies/hybrid-threats/.
[34] Al Aridi, *supra note*, 9: 9.

nekonvencinių metodų (diplomatinių, ekonominių, karinių, technologinių) derinį, kurį gali naudoti valstybiniai ar nevalstybiniai veikėjai, siekdami konkrečių tikslų, tačiau išlikdami žemiau oficialiai paskelbto karo ribos.[35]

Hibridinių grėsmių pagrindinis tikslas - prievartine ir ardomąja veikla, naudojant konvencinius (karinius) ir nekonvencinius (technologinius, ekonominius ir diplomatinius) metodus, siekti specifinių tikslų, neskelbiant tiesioginio karo kitai valstybei.[36] Piktybiniai veikėjai naudoja įvairias technikas, jų taikiniu sąmoningai yra pasirenkamos pažeidžiamiausios valstybės vietos. Veiksmais siekiama pažeisti saugumą, daryti įtaką sprendimų priėmimui, destabilizuoti demokratinių institucijų veiklą.[37]

E. Štareikė hibridines grėsmes apibūdina kaip karinius ir nekarinius, atvirus ir slaptus veiksmus, kuriuos nevalstybiniai veikėjai koordinuotai naudoja siekdami konkrečių tikslų, tačiau neperžengiant formaliai skelbiamo karo ribos. Hibridiniai metodai yra naudojami tam, kad ribos tarp karo ir taikos būtų ištrintos, o visuomenė destabilizuota ir nusilpusi.[38]

Anot Patryk Pawlyk, hibridinės grėsmės yra metafora, apibūdinanti iššūkius ir dilemas, kurios kyla dėl nuolat besikeičiančios tvarkos pasaulyje. Šis terminas dažnai naudojamas kartu su hibridinio karo terminu, norint apibrėžti tarpusavyje susijusių iššūkių įvairovę.[39] Straipsnio autorius, teigia, kad hibridines grėsmes, hibridinį konfliktą ir hibridinį karą, galima atskirti atsižvelgiant į skirtingą grėsmės intensyvumo lygį, konflikto dalyvius ir jų veiksmus:

Hibridinės grėsmės - reiškinys, atsirandantis dėl skirtingų elementų susikirtimo ir tarpusavio ryšio, kurie kartu sudaro sudėtingesnę ir daugialypę grėsmę. Hibridinis konfliktas ir hibridinis karas yra dvi specifinės kategorijos, kuriose valstybė naudoja tam tikrą hibridinę taktiką savo strateginiams tikslams pasiekti.[40]

Hibridinis konfliktas - padėtis, kuomet šalys susilaiko nuo atviro ginkluotųjų pajėgų panaudojimo viena prieš kitą. Vietoje to, šalys remiasi kariniu bauginimu, ekonominiu ir politiniu pažeidžiamumu, taip pat diplomatinių ir technologinių priemonių visuma, savo tikslui pasiekti.[41]

Hibridinis karas - situacija, kurios metu, yra atvirai naudojamos šalies ginkluotosios pajėgos, kartu įtraukiant ekonomines, diplomatines ir technologines priemones.[42]

---

[35] Seniutienė, Paulauskytė, *supra note*, 10: 195–202.
[36] Cirdei, Ispas, *supra note*, 4: 72.
[37] Lisboa, *supra note*, 7: 1.
[38] Štareikė, *supra note*, 11: 229.
[39] Patryk Pawlak „Understanding hybrid threats", European Parliament, žiūrėta 2025 m. lapkričio 14 d., https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/.
[40] *Ibid*.
[41] *Ibid*.
[42] *Ibid.*

Hibridinių grėsmių ir hibridinio karo sąvokos, Sean Monaghan teigimu, dažnai yra sutapatinamos, tačiau tai yra du skirtingi dalykai. Hibridinio karo sąvoka apibūdina karo pobūdžio pasikeitimą, kuomet yra kombinuojamos tiek karinės, tiek nekarinės priemonės.[43]

Hibridinio karo samprata yra labai glaudžiai susijusi su ketvirtosios kartos karo koncepcija, kurios esmė – propaganda per viešas informavimo priemones, teroristiniai veiksmai, ekonominių, finansinių, energetinių, socialinių ir karinių spaudimo priemonių naudojimas. Minėtais veiksmais yra išnaudojamas šalies pažeidžiamumas, siekiama paveikti ar destabilizuoti, trukdyti sprendimų priėmimui ir taip pasiekti išsikeltus uždavinius.[44] *„Ketvirtos kartos karu vadinamas konfliktas, kai santykis tarp karinių ir politinių priemonių neapibrėžtas, sąsajos tarp kovotojų ir civilių visiškai neaiškios.[...] Tokiame kare dominuoja ne valstybė, bet nevalstybiniai ginkluoti dariniai (sukilėliai ar pan).“*[45] Ketvirtosios kartos karo pavyzdžių laikoma Krymo aneksija ir Rusijos intervencija į Ukrainą.[46]

Hibridinės priemonės yra sąmoningai kuriamos taip, jog sukeltų sumaištį, o tikrieji ketinimai liktų neatskleisti. Dėl šios priežasties, tokio tipo veikas būtina vertinti ne kaip pavienius incidentus, tačiau kompleksines grėsmes, kurios tuo pačiu metu gali veikti skirtingose srityse. Norint nustatyti tikrąjį hibridinės atakos tikslą, taip pat labai svarbu įvertinti ir hibridinio veikėjo geopolitinį kontekstą, kultūrines ypatybes bei kitus veiksnius.[47]

Lyginant konvencinio ir nekonvencinio karo bruožus, Thomo R. Mockaičio teigimu, konvencinis karas referuoja į konfliktą tarp įprastų ginkluotųjų pajėgų, kurios dėvi savo uniformą ir yra išsidėsčiusios aiškia fronto linija. Nekonvencinis karas, autoriaus apibūdinamas, kaip kitokių nei konvencinio karo veiksmų įvairovė. Šių laikų mokslininkai sugalvojo terminą „asimetrinis karas”, kadangi labai dažnu atveju nekonvenciniame kare kariaudavo vyriausybių nekontroliuojamos grupuotės, kurios jokiais tradiciniais kariavimo būdais negalėdavo tikėtis įveikti šalies ginkluotasias pajėgas.[48]

Išanalizavus įvairių mokslininkų akademinius darbus, darytina išvada, kad hibridinių grėsmių reiškinys yra sunkiai apibrėžiamas dėl savo kompleksiškumo, tačiau sutinkama, kad hibridinės grėsmės laikomos prievartinių ir ardomųjų veiklų, konvencinių ir nekonvencinių

---

[43] Sean Monoghan „Countering Hybrid Warfare”, *Features* 8, 2, (2019): 86, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf?ver=2019-09-17-231051-890.

[44] Bajarūnas, Keršanskas, *supra note,* 8: 129.

[45] Vitalijus Leibenka, „Ketvirtosios kartos karas“, *Kultūros barai 10, (2019)*: 2-7, https://etalpykla.lituanistika.lt/object/LT-LDB-0001:J.04~2018~1615394203071/J.04~2018~1615394203071.pdf.

[46] *Ibid.*

[47] Rita Costa, *Hybrid threats in the context of European security*, (National Defense Instituce of Portugal, 2022), 2, https://comum.rcaap.pt/bitstream/10400.26/37389/1/COSTARita_HybridthreatsincontextofeuropeansecurityE_BriefinsPapers_Maio_2021.pdf.

[48] Thomas R. Mockaitis, *Conventional and Unconventional War – A history of Conflict in the Modern World*, Bloomsbury Publishing USA, 2017, 9-10.

metodų derinys, naudojamas valstybinių ar nevalstybinių subjektų, siekiančių priešiškų tikslų, tačiau neskelbiant karo ir išliekant žemiau oficialaus karo ribos. Šiomis priemonėmis siekiama destabilizuoti padėtį valstybėje, sukelti visuomenes abejones valstybinių institucijų darbu, didinti nesaugumo jausmą. Riba, tarp konvencinio ir hibridinio karo yra labai plona, tačiau sutinkama, jog konvencinį karą nuo hibridinio karo skiria tiesioginės karinės jėgos ir priemonių panaudojimo elementas, o kova su hibridinėmis grėsmėmis yra nuolatinis ir nesibaigiantis procesas.

1.2 Hibridinių grėsmių rūšys ir „pilkoji zona“

Hibridinių grėsmių sampratos esminių pokyčių pastaraisiais metais nepastebima, tačiau dėl globalizacijos, technologinių ir geopolitinių pokyčių, hibridinėms atakoms naudojamų priemonių ir metodų pobūdis, veikimo laukas, nuolat keičiasi ir plečiasi.[49] Įvertinus tai, tikslinga nustatyti pagrindines hibridinių grėsmių rūšis.

Lietuvos Respublikos Prezidentas Gitanas Nausėda 2025 metų spalio mėnesį vykusioje strateginės politikos konferencijoje, teigė, kad *,,Mums niekas nepaskelbė karo, tačiau mes, kaip bendruomenė, atsidūrėme pačiame konflikto įkarštyje. Tradicinės ribos tarp karo ir taikos nyksta, jas keičia pilkoji zona. Joje įvairūs nedraugiškų valstybių remiami veikėjai pasitelkia visą virtinę karinių ir nekarinių priemonių, kurios daro žalą, bet nesulaukia ginkluoto atsako*“.[50]

Analizuojant hibridinių grėsmių rūšis, labai svarbi anksčiau minėta, ,,vadovėliniu“ hibridinio karo pavyzdžių laikoma, Krymo pusiasalio okupacija. Pirmieji Rusijos hibridinių grėsmių požymių turintys veiksmai pasireiškė 2014 metais, kuomet Rytų Ukrainoje pasirodė gerai ginkluoti ir apmokyti vyrai, pradėję organizuoti demonstracijas, periminėti savivaldos pastatus, policijos komisariatus, prisidengdami vietinių separatistų, nepatenkintų esama valdžia, vardu. Lygiagrečiai šiems veiksmams, kartu buvo naudojamas ir diplomatinis, ekonominis spaudimas, skleidžiama dezinformacija Ukrainos ir užsienio žiniasklaidose, kas dar labiau apsunkino Ukrainos suverenumo ir teritorijos vientisumo išsaugojimą. To pasekoje, separatistų grupuotėms pavyko nutraukti tuometinės valdžios darbą Krymo pusiasalyje ir pilnai jį aneksuoti nepanaudojus jokio smurto. Rusijos veiksmuose prieš Ukrainą nebuvo aiškiai išreikšto konkretaus priešo, įvairias diversijas Ukrainoje vykdė „žalieji žmogeliukai“ (diversantai) be skiriamųjų ženklų. Be

[49] Ugnė Alaburdaitė, „Hibridinių grėsmių prevencijos teisinė sistema“ (magistro baigiamasis darbas, Mykolo Romerio universitetas, 2025, 12, https://www.lvb.lt/permalink/370LABT_NETWORK/cdhmhi/alma9917024127908451.

[50] „Lietuvos Respublikos Prezidento Gitano Nausėdos kalba strateginės politikos konferencijoje „Universitetai, formuojantys ateitį: atsparios visuomenės kūrimas per inovacijas ir visuotinį poveikį“, Lietuvos Respublikos Prezidentas, žiūrėta 2025 m. lapkričio 15 d., https://lrp.lt/lt/lietuvos-respublikos-prezidento-gitano-nausedos-kalba-strategines-politikos-konferencijoje-universitetai-formuojantys-ateiti-atsparios-visuomenes-kurimas-per-inovacijas-ir-visuotini-poveiki/46153.

kita ko, Ukraina buvo veikiama naudojant ir diplomatinį, ekonominį ir energetinį spaudimą, kibernetines atakas, kol galiausiai viskas pasisuko konvencinio karo keliu.[51]

Susana Sanz-Caballero savo moksliniame straipsnyje nurodo, kad hibridinės grėsmės apima ne vien akivaizdžiai neteisėtus veiksmus, tačiau ir neetišką elgesį ar kitokias veikas. Vertinant šią aplinkybę, darytina išvada, kad bet kokie veiksmai, susiję su valstybės ir jos visuomenės destabilizavimu yra vykdomi „pilkojoje zonoje“ ir gali būti vertintini kaip hibridinė grėsmė. Mokslininkė taip pat pateikia labai platų hibridinių grėsmių sąrašą, pradedant nuo politinės veiklos, dezinformacijos, kibernetinių atakų, terorizmo, baigiant migracija, narkotikų prekyba, dronais ir orlaivių ar laivų užgrobimu. Šiandieniniame pasaulyje, bet kuri grėsmė gali tapti hibridinė, nes jų pobūdis nuolat kinta, išskyrus tuos atvejus, kai yra paskelbtas oficialus karas.[52]

Po žodžiu „hibridinis“ stengiamasi įtalpinti viską, kas vyksta nekonvencine forma arba yra sunkiai apibrėžiama tradiciniais terminais. E. Bajarūnas pažymi, kad net ir protestuojantys darbininkai, gali būti priskiriami prie hibridinės atakos.[53] Esant tokiam dideliam hibridinių grėsmių reiškinio neapibrėžtumui, valstybės susiduria su tokio tipo grėsmių atrėmimo ir priemonių taikymo problema.

Mokslininkai Ionutas Cirdei ir Lucia Ispas taip pat aprašė pagrindines hibridinių grėsmių rūšis, keliančias pavojų valstybei ir jos gyventojams, tačiau pažymėtina, kad sąrašas nėra baigtinis.[54] (žr. 1 lent.)

1 lentelė. Hibridinių grėsmių rūšys

Hibridinių grėsmių rūšys
1. Dezinformacija visuomenės informavimo priemonėse
2. Parama suinteresuotoms nevyriausybinėms organizacijoms
3. Kontroliuojami gamtiniai ištekliai ir jų kainos
4. Spaudimas įstatymų, naudingų tam tikroms interesų grupėms, leidybai
5. Kenkimas pagrindinėms valstybės ekonomikos sritims
6. Poveikis didelėms emigrantų grupėms, jų kontrolė
7. Strateginių objektų kontrolė ginkluotomis grupuotėmis, kurios neturi aiškios priklausomybės

[51] Bajarūnas, Keršanskas, *supra note,* 8*:* 128.
[52] Susana Sanz-Caballero, „The concepts and laws applicable to hybrid threats, with a special focus on Europe“, *Humanities and Social Sciences Communications*, 10, 360 (2023): 2, https://doi.org/10.1057/s41599-023-01864-y.
[53] Bajarūnas, Keršanskas, *op.cit*., 9: 129-130.

Hibridinių grėsmių rūšys
8. Nuomonės poveikis didelėms asmenų grupėms
9. Kibernetinės atakos
10. Parama streikų ir demonstracijų organizatoriams
11. Teikiama parama etninėms mažumoms, disidentams
12. Geriamo vandens, maisto užteršimas
13. Įvairios diversijos, atakos
14. Įtakingų asmenų poveikis, panaudojant šantažą, korupciją
15. Kitos grėsmės

Šaltinis: sudaryta darbo autoriaus, remiantis Ionut Alin Cirdei, Lucian Ispas.[55]

Atsižvelgiant į pateiktas hibridinių grėsmių rūšis, galima teigti, kad vyrauja tam tikra pagrindinė jų klasifikacija: 1) kibernetinės atakos; 2) diplomatinis spaudimas; 3) propaganda visuomenės informavimo priemonėse; 4) terorizmas; 5) įvairios diversijos, išpuoliai; 6) kenkimas svarbiausioms ekonomikos sritims.

Hibridinėse grėsmėse yra eliminuojamas smurto elementas, bandoma išvengti atsakomųjų veiksmų, o naudojamos priemonės patenka į taip vadinamąja „pilkąją zoną" - neapibrėžtumą tarp taikos ir karo.[56]

Mokslininkai, „pilkąją zoną" apibūdina, kaip konkuruojančių valstybinių ir nevalstybinių veikėjų tarpusavio sąveikas, kurios vyksta tarp įprastinių karo ir taikos būsenų. Tokiems veiksmams būdingas neaiškus konflikto pobūdis, dalyvaujantys veikėjai, taip pat politinio ir teisinio reguliavimo rėmų taikymo neapibrėžtumas. Tokioje erdvėje besikaupiantys įvairūs konfliktai, palaipsniui lemia tam tikros valstybės destabilizaciją.[57] Riba tarp išpuolių, kurie gali būti laikomi karo veiksmais, ir tų, kurie tokiais nelaikytini, nėra aiškiai nubrėžta, todėl jos neįmanoma tiksliai reglamentuoti jokiomis teisės normomis. Teisėje nėra įtvirtintas aiškus atsakymas ar apibrėžimas apie tokius ribinius atvejus, dėl jų kvalifikacijos kaip karo veiksmų. Tokiais atvejais klausimas, ar išpuolis laikytinas karo veiksmu, tampa politinis, o ne teisinis, o atsakymas priklauso nuo politinių sprendimų, kuriuos priima užpulta valstybė.[58] NATO lygmeniu

[55] Cirdei, *supra note*, 4: 116.
[56] Monoghan, *op.cit., 86.*
[57] Leszek Sykulski, „Old Methods in the New Framework". Strategy of Grey Zones in Hybrid Warfare, Strategies XXI – National Defence College", *Proceedings 2021 „Romania and the new dynamics of international security"* 1, 72 (2021): 163, https://doi.org/10.53477/2668-5094-21-11.
[58] Jan Almäng, „War, Vagueness and Hybrid War", Defence Studies 19, 2 (2019): 193, https://www.tandfonline.com/doi/epdf/10.1080/14702436.2019.1597631?needAccess=true.

jau pradėta sutarti, jog hibridinė grėsmė apima *„viską, kas yra iki NATO Penktojo straipsnio“*[59], todėl hibridinė grėsmė negali būti prilyginama konvencinės karinės galios panaudojimui.[60] Iš to galime daryti išvadą, jog konvencinį karą nuo hibridinio karo skiria tiesioginės karinės jėgos panaudojimo elementas.

Kalbant apie hibridinių grėsmių rūšis, daugialypiškumą ir kitimą, bendrąja prasme, net ir teisė, gali būti panaudota ne tik žmogaus teisių gynybai, tačiau ir kaip hibridinės atakos priemonė. Valstybiniai arba nevalstybiniai subjektai teisę naudoja kaip priemonę savo strateginiams tikslams įgyvendinti. Hibridinės grėsmės požiūriu teisę geriausiai suprasti ir kaip instrumentą, ir kaip strateginės konkurencijos sritį.[61] 2010 metais NATO atliko koncepcinį tyrimą, kuriuo nustatė kelis teisinius iššūkius, kuriuos sukelia hibridinės grėsmės. Vienas iš jų - priešiškų veikėjų naudojimasis teisine sritimi, siekiant sutrikdyti valstybių vykdomas operacijas.[62] Kaip viena iš hibridinių grėsmių panaudojimo galimybių, yra įvardijama „lawfare” (liet. teisinis karas). Vieną pirmųjų šio reiškinio apibrėžimų pateikė Jungtinių Amerikos Valstijų karininkas Charles J. Dunlap, kuris tai apibūdino kaip tinkamą arba netinkamą teisės panaudojimo strategiją vietoje įprastų teisinių priemonių, siekiant įgyti tam tikrą pranašumą.[63] Šis apibrėžimas buvo praplėstas, kaip realių, suvokiamų ar inscenizuotų karo teisės pažeidimų išnaudojimas, kaip netradicinė priemonė kariaujant su pranašesne karine jėga.[64] Vienas iš tokių pavyzdžių, Europos Žmogaus teisių teismui pateikti keli tūkstančiai ieškinių iš Rusijoje ir ginčijamose Rytų Ukrainos teritorijose įsikūrusiu teisininkų ir įmonių, kurie kaltino Kijevo valdžią žmogaus teisių pažeidimais Donbase.[65]

Apibendrinant, pagrindinės naudojamos hibridinių grėsmių rūšys yra diplomatinis, ekonominis spaudimas, kibernetinės atakos, propaganda, įvairios diversijos, išpuoliai, kenkimas svarbiausioms ekonomikos sritims. Šių priemonių naudojimas, patenka į „pilkąją zoną“, kurioje riba tarp išpuolių, kurie gali būti laikomi karo veiksmais, ir tų, kurie tokiais nelaikytini, nėra aiškiai nubrėžta, nėra žinomas konkretus išpuolių vykdytojas, viskas vyksta neskelbiant oficialaus karo. Atsižvelgiant į tai, valstybėms ir jų institucijoms kyla sunkumų atsakant į tokio tipo hibridinius išpuolius.

---

[59] *Autoriaus pastaba: NATO sutarties 5 straipsnis - „Šalys susitaria, kad vienos ar kelių iš jų ginkluotas užpuolimas Europoje ar Šiaurės Amerikoje bus laikomas jų visų užpuolimu [...]*“, „Šiaurės Atlanto sutartis“, NATO, žiūrėta 2026 m. gegužės 1 d., https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty?selectedLocale=lt.

[60] Matonytė, Gajauskaitė, Denisenko, *supra note,* 19: 21.

[61] *Ibid,* 41.

[62] Aurel Sari „Hybrid threats and the law: Building legal resilience”, *Hybrid CoE Research, Report 3*, (2021): 9, https://www.hybridcoe.fi/publications/hybrid-coe-research-report-3-hybrid-threats-and-the-law-building-legal-resilience/.

[63] Zakhar Tropin, „Lawfare as part of hybrid wars: The experience of Ukraine in conflict with Russian Federation”, Security and Defence Quarterly, 33, 1, 2021, https://doi.org/10.35467/sdq/132025.

[64] *Ibid*.

[65] Sari, *op.cit*., 30.

1.3 Nacionalinio saugumo samprata ir sąsajos su hibridinėmis grėsmėmis

Lotynų kalboje, žodis saugumas – *securitas,* kildinamas iš dviejų dedamųjų dalių: sine (be) ir cura (susirūpinimas, nerimas, baimė), kas pažodžiui reiškia baimės, nerimo nebuvimą. Senovės Romoje, tai buvo laikoma politiniu valstybės stabilumu, tvarkos palaikymu. Nacionalinio saugumo samprata iš pradžių buvo labai glaudžiai susijusi su geografiškai apibrėžtos teritorijos - valstybės saugumu ir gynyba nuo išorinių ir vidinių grėsmių, siekiant apsaugoti šalį nuo išnykimo.[66] Vis dėl to, pasibaigus Šaltojo karo laikotarpiui, valstybių viduje kylančių konfliktų skaičiaus augimas, imigracija ir įvairios pandemijos privertė praplėsti saugumo sampratos ribas. Nuo tradicinės politinio-militaristinio saugumo sampratos, kuri buvo susikoncentravusi ties valstybe ir jos suvereniteto išsaugojimu, buvo pereita prie holistinio požiūrio į taiką, tarptautinį stabilumą, paremtą individų apsauga.[67] Šių laikų visuomenėje saugumas yra laikomas kaip taikos, grėsmių nebuvimo ir užtikrintumo būsena.[68] Lietuvos mokslininkų akimis, *„didėjant grėsmių nacionaliniam saugumui spektrui, didėja ir Lietuvos visuomenės nerimas dėl konvencinių ir hibridinių grėsmių žalos. [...]”.*[69]

Akademiniame pasaulyje, valstybės nacionalinio saugumo sąvoką gali būti suprantama ir vartojama skirtingame kontekste, nei kasdieniame gyvenime, todėl konkrečiai apibrėžti ir įstatyti jos į rėmus yra pakankamai sudėtinga. Įprastai, ši sąvoka reiškia valstybės suvereniteto išsaugojimą panaudojant turimas politines, karines ir diplomatines galias, gynybos priemones nuo išorės priešų ar kitų grėsmių, bei valstybės paslapčių saugojimą.[70] Saugumo koncepcija įprastai žymi nacionalinio saugumo, gynybos sistemų prisitaikymą ir reakciją į vidaus ir išorės iššūkius bei grėsmes. Grėsmių nacionaliniam saugumui suvokimą ir jo pasikeitimus daugiausiai lemia politinė sistema, istorinė atmintis, nacionaliniai interesai, jų kaita ir saugumo identitetas.[71]

Nacionalinis saugumas taip pat gali būti suprantamas kaip vyriausybės galimybė panaudoti karinę jėgą, siekiant apsaugoti šalies gyventojų saugumą, ekonominę gerovę ir institucijas nuo vidinių ir išorinių grėsmių.[72]

---

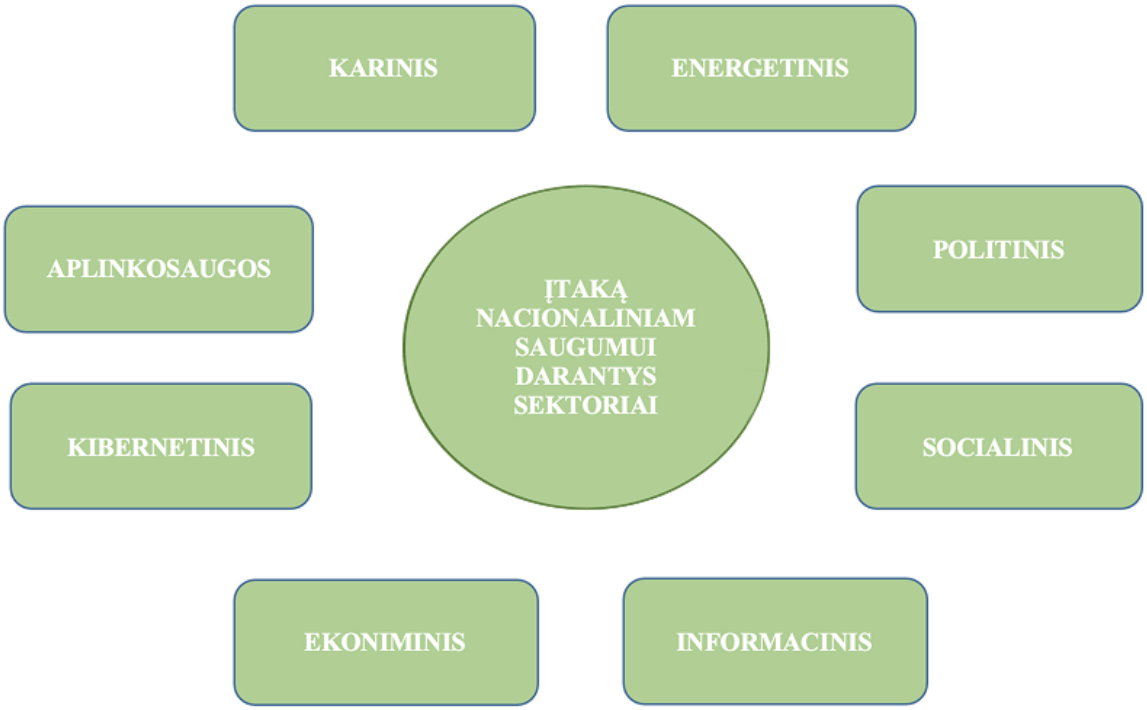
[66] Christian Fjader, „The nation-state, national security and resilience in the age of globalisation”, *Resilience* 2, 2 (2014): 117, https://doi.org/10.1080/21693293.2014.914771.
[67] Joao Estevens, „Migration crisis in the EU: developing a framework for analysis of national security and defence strategies”, *Estevens Comparative Migration Studie* 6, 28 (2018): 3, https://link.springer.com/article/10.1186/s40878-018-0093-3.
[68] Henryk Wyrebek, „National security challanges and threats”, *Wiedza Obronna* 279, 2 (2022): 2, https://doi.org/10.34752/2022-e279.
[69] Irmina Matonytė, Ieva Gajauskaitė ir Matas Jasinavičius, „Hibridinės grėsmės Lietuvoje: sampratos žinomumas ir raiškos formų atpažinimas jaunimo tarpe”, Viešoji politika ir administravimas, 23, 3 (2024): 357, https://doi.org/10.5755/j01.ppaa.23.3.35169.
[70] Kazlauskaitė-Markelienė, Petrauskaitė, *supra note*, 15: 237.
[71] Karpavičiūtė, *supra note*, 17: 10.
[72] Kaplan, *supra note*, 12: 400.

R. Kazlauskaitės-Markelienės ir A. Petrauskaitės nuomone, *„Lietuvos nacionalinis saugumas yra suprantamas, kaip Tautos ir valstybės laisvos ir demokratinės raidos sąlygų sudarymas, Lietuvos valstybės nepriklausomybės, jos teritorinio vientisumo ir konstitucinės santvarkos apsauga ir gynimas".*[73]

Nacionalinio saugumo užtikrinimas susideda iš tikslingų ir kryptingų visuomenės ar valstybės veiksmų, kurių pagrindinis tikslas - užtikrinti valstybės suverenitetą, konstitucinę tvarką, vystyti gerovės valstybę. Tokie veiksmai apima daugelį žmogaus gyvenimo sričių, todėl siekiant efektyvumo, atsiranda poreikis išskirti jų pagrindines kryptis.[74] S. Greičius ir B. Pranevičienė pateikė penkis pagrindinius, tarpusavyje susijusius nacionalinio saugumo sektorius, kuriuose atsiradus grėsmėms, pakilęs nesaugumo lygis turi įtakos valstybei ir visuomenei. Pažymėtina, kad pastaraisiais metais saugumo sektorių sąrašas dėl vykstančios technologinės raidos, buvo praplėstas informacinio ir kibernetinio saugumo sektoriais.[75] Autorių teigimu „*[...] individualaus saugumo lygis daro įtaką ir nacionaliniam saugumui: valstybėje, kurioje piliečiai jaučiasi nesaugūs, konfliktuoja su valstybe, susiklosčiusi vidinė tvarka, arba tiksliau, netvarka, gali kelti grėsmę ir nacionaliniam saugumui*".[76] Kitas mokslininkas, A. M. Nebo nurodo, jog nacionalinis saugumas pasipildė tokiomis sritimis, kaip apsauga nuo terorizmo, nusikalstamumo mažinimu, ekonominiu, energetiniu ir kibernetiniu saugumu.[77] (žr. 2 lent.)

[73] Kazlauskaitė-Markelienė, Petrauskaitė, *op.cit.,* 15: 238.
[74] Bileišis, Ungurytė-Ragauskienė, *supra note*, 18: 32.
[75] Isoda, *supra note*, 16: 8.
[76] Greičius, Pranevičienė, *supra note*, 14: 722.
[77] Nebo, *supra note*, 13: 396.

2 lentelė. Įtaką nacionaliniam saugumui darantys sektoriai



Šaltinis: Sudaryta darbo autoriaus, remiantis S. Greičiumi, B. Pranevičiene, V. Isoda ir A. M. Nebo.

Lietuvos Respublikos Nacionalinio saugumo strategijoje, priimtoje 2021 metais nurodoma, kad Lietuvos Respublika savo nacionalinį saugumą suvokia, kaip „*sutelktomis Lietuvos valstybės ir piliečių pastangomis vykdomą valstybingumo ir demokratijos plėtrą bei stiprinimą, Tautos saugaus būvio ir valstybės vidaus bei išorės saugumo užtikrinimą, kiekvieno potencialaus užpuoliko atgrasymą, Lietuvos Respublikos nepriklausomybės, teritorijos vientisumo ir konstitucinės santvarkos gynimą*”.[78]

Kalbant apie užsienio valstybių, o būtent Rusijos hibridinę veiklą, keliančią grėsmę Lietuvos nacionaliniam saugumui, aktualus 2024 m. gegužės 9 d. Vilniuje, baldų parduotuvės „Ikea” sandėlyje kilęs gaisras. Lietuvos Generalinė prokuratūra patvirtino, kad gaisro priežastis buvo parduotuvės sandėlyje padėtas sprogmuo, o išpuolį įvykdė du Rusijos tarnybų užverbuoti Ukrainos piliečiai, iš kurių vienas nepilnametis. Generalinės prokuratūros vyriausiasis prokuroras Arūnas Urbelis teigė, kad *„surinkti duomenys leido mums padaryti išvadas, kad šių veiksmų organizatoriai yra Rusijoje, tai susiję su karine žvalgyba, saugumo pajėgomis”.*[79] Panašūs išpuoliai turėjo būti įvykdyti ne tik Lietuvoje, tačiau ir Latvijoje. Jog Rusijos specialiosios tarnybos nuolat ieško naujų priemonių ir būdų paveikti paveikti visuomenės pasitikėjimą

[78] „Dėl Nacionalinio saugumo strategijos patvirtinimo”, TAR žiūrėta 2026 m. sausio 19 d., https://www.e-tar.lt/portal/tt/legalAct/TAR.2627131DA3D2/asr.
[79] „Ikea“ padegimo byla: kruopščiai rengtas tarptautinis Rusijos teroro aktas, Delfi, žiūrėta 2026 m. sausio 19 d., https://www.delfi.lt/news/daily/lithuania/ikea-padegimo-byla-kruopsciai-rengtas-tarptautinis-rusijos-teroro-aktas-120094314.

teisėsaugos institucijomis, didinti gyventojų nerimą, baimę ir įtampą įvairiais išpuoliais rodo ir Lietuvos kriminalinės policijos biuro atliktas ikiteisminis tyrimas, kurio metu buvo sulaikyta asmenų grupė, organizavusi ir planavusi įvykdyti keturis teroro aktus, turinčius hibridinių tikslų. Ikiteisminio tyrimo metu nustatyta, kad 2024 m. liepos mėn. Lietuvos pilietis veikdamas kartu su bendrininkais, naudodamasis „DHL" ir „DPD" siuntų bendrovėmis, iš Vilniaus į įvairias Europos valstybes išsiuntė keturias siuntas, kuriose buvo savadarbiai sprogstamieji-padegamieji užtaisai. Trys iš keturių siuntų savaime užsidegė jas transportuojant Vokietijoje, Lenkijoje ir Jungtinėje Karalystėje. Ketvirtoji, dėl techninio gedimo nesuveikė. Atsižvelgiant į tyrimo svarbą ir nusikaltimų sunkumą, buvo įkurta jungtinė tyrimo grupė, kurioje glaudžiai bendravo daugelis Europos valstybių teisėsaugų ir žvalgybos institucijų. Ikiteisminio tyrimo metu buvo nustatyta, kad nusikaltimus organizavo Rusijos Federacijos piliečiai, turintys ryšių su Rusijos karinės žvalgybos tarnybomis. Be kita ko, buvo nustatyta, kad tie patys asmenys yra tiesiogiai susiję ir su anksčiau minėtu „Ikea" prekybos centro padegimu. Įtarimai iš viso buvo pareikšti 15 asmenų.[80] Prezidento Gitano Nausėdos patarėjas nacionalinio saugumo klausimais Kęstutis Budrys komentavo, jog pastarojo meto Rusijos sabotažo atvejai negali būti palikti be atsako ir būtina NATO lygmeniu kelti klausimus dėl valstybių narių teritorijose vykdomų Rusijos nekonvencinių operacijų.[81] Taigi, Rusijos vykdomi hibridiniai išpuoliai siekia paveikti visuomenės saugumo jausmą, pasitikėjimą valstybinėmis institucijomis, didinti nerimą ir baimę, mažinti gyventojų palaikymą ir jų paramą Ukrainai. Tokio tipo atakos organizuojamos tarptautiniu mastu, o sėkmingas jų ištyrimas ir kitų hibridinių grėsmių užkardymas įmanomas tik tarpusavyje bendradarbiaujant su kitomis Europos valstybių institucijomis. Panašių hibridinių atakų pavyzdžių yra dar daugiau, tiek Lietuvoje, tiek ir kitose Europos valstybėse.

Hibridinės atakos prieš Lietuvą rengiamos ne vien fizinėje, tačiau ir elektroninėje erdvėje. 2026 metų balandžio 8 d. Valstybės saugumo departamentas paskelbė, jog tarptautinėje operacijoje, kartu su Jungtinių Amerikos Valstijų Federalinių tyrimų biuro pareigūnais, neutralizavo kibernetinę grupuotę, kuri buvo siejama su Rusijos karinės žvalgybos tarnyba (GRU), kuri sistemingai išnaudojo namų ir įmonių maršrutizatorius, pakeičiant nustatymus ir nukreipiant interneto srautą per jų valdomą infrastruktūrą. Tokiu būdu, buvo renkama jautri informacija apie elektroninio pašto turinį ir įvairius prisijungimo duomenis. Ataka vykdyta plačiu mastu nuo 2024

[80] „Išaiškinta ir sulaikyta asmenų grupė, organizavusi ir planavusi įvykdyti keturis teroro aktus, turinčius hibridinių tikslų", Lietuvos Policija, žiūrėta 2026 m. balandžio 15 d., https://policija.lrv.lt/lt/naujienos/isaiskinta-ir-sulaikyta-asmenu-gruoe-organizavusi-ir-planavusi-ivykdyti-keturis-teror-aktus-turincius-hibridiniu-tikslu-0hsd/.

[81] „Iš Lietuvos į Vokietiją ir JK savaime užsidegančias siuntas galėjo siųsti Rusija", Verslo žinios, žiūrėta 2026 m. balandžio 15 d., https://www.vz.lt/verslo-aplinka/2024/11/05/is-lietuvos-i-vokietija-ir-jk-savaime-uzsidegancias-siuntas-galejo-siusti-rusija.

metų. Jos metu buvo pasirenkami konkretūs taikiniai, susiję su gynybos sektoriumi, valstybės institucijomis ir kritine infrastruktūra.[82]

Apibendrinant, galima teigti, kad šalies nacionalinis saugumas yra suprantamas, kaip valstybės teritorijos, suvereniteto ir jos gyventojų apsauga nuo išorinių ir vidinių grėsmių. Tai yra prioritetinė valstybės ir jos institucijų veiklos sritis, reikalaujanti ypatingo dėmesio, išteklių ir nuoseklios, ilgalaikės strategijos. Nacionaliniam saugumui įtaką daro aplinkosaugos, kariniui, ekonominiui, socialiniui, energetiniui ar politiniui valstybės sektoriams kylančios grėsmės. Hibridinės atakos prieš Lietuvos valstybę yra vykdomos ir tai tiesiogiai veikia šalies nacionalinį saugumą. Tokie išpuoliai siekia paveikti visuomenės saugumo jausmą, pasitikėjimą valstybinėmis institucijomis, didinti nerimą ir baimę.

[82] „VSD: Rusijos GRU svetur naudojosi pažeidžiamais maršrutizatoriais vogti slaptą informaciją“, Lietuvos nacionalinis radijas ir televizija, žiūrėta balandžio 8 d., https://www.lrt.lt/naujienos/pasaulyje/6/2892299/vsd-rusijos-gru-svetur-naudojosi-pazeidziamais-marsrutizatoriais-vogti-slapta-informacija.

2. EUROPOS SĄJUNGOS, NATO IR LIETUVOS SAUGUMO STRATEGIJOS KOVOJANT SU HIBRIDINĖMIS GRĖSMĖMIS

Nors pirminis atsakas į hibridines grėsmes iš pradžių yra nacionalinio lygmens valstybės pareiga, visgi jų prigimtis reikalauja glaudaus valstybių bendradarbiavimo su sąjungininkais ir kitais partneriais.[83] Europoje kilus hibridinių grėsmių problemai, Europos Sąjungai kilo būtinybė peržiūrėti tradicinį saugumo suvokimą ir imtis daugiau saugumo priemonių. 2014 metais Europos Komisijos prezidentas Jean-Claude Juncker išreiškė didelį susirūpinimą ir savo politinėse gairėse išsikėlė tikslą „*dirbti dėl stipresnės Europos, saugumo ir gynybos srityje*".[84] Hibridinių grėsmių politinės krypties formavimosi pradžia Europoje, gali būti laikomi 2015 metai, kada Europos išorės veiksmų tarnybos (angl. EEAS) parengtame informaciniame dokumente, skirtame kovai su hibridinėmis grėsmėmis buvo konstatuota, kad *„nei ES, nei NATO šiuo metu neturi strategijos, kaip kovoti su hibridinėmis grėsmėmis"*[85]. Žemiau bus analizuojamos Europos Sąjungos parengtos ir įgyvendinamos priemonės, bei strategijos, skirtos kovoti su hibridinėmis grėsmėmis, taip pat aptariamas ES ir NATO bendradarbiavimas, jų įgyvendinamos priemonės.

2.1 Europos Sąjungos atsakas į hibridines grėsmes

2016 m. balandžio mėnesį buvo žengtas pirmasis Europos Sąjungos (toliau ES) žingsnis kovoje su hibridinėmis grėsmėmis. Europos Komisija priėmė **„Bendros sistemos, kovojant su hibridinėmis grėsmėmis" komunikatą**, kurio paskirtis koordinuotas Europos Sąjungos šalių atsakas į kylančias grėsmes, ypatingą dėmesį skiriant taikai ir stabilumui rytinėje ir pietinėje Europos dalyse, derinant skirtingas priemones ir skatinant šalių tarpusavio bendradarbiavimą.[86] Komunikate buvo pateiktas ir būtinų imtis priemonių sąrašas:

1) atlikti hibridinių grėsmių rizikos vertinimą, siekiant nustatyti labiausiai pažeidžiamas valstybių narių vietas;

2) hibridinių grėsmių analizės skyriaus įkūrimas, skirtas informacijos dalijimuisi tarp valstybių narių, hibridinių grėsmių klausimais;

3) strateginės komunikacijos atnaujinimas ir jos koordinavimas;

---

[83] Vytautas Keršanskas, „Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats", *The European Centre of Excellence for Countering Hybrit Threats,* 2020: 8, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.

[84] European Commision, Joint communication to the european parliamant and the council. Joint Framework on contering hybrid threats (JOIN(2016) 18 final, 2016 m. birželio 4 d.), žiūrėta 2026 m. sausio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52016JC0018.

[85] Council of the European Union, „*Food-for-thought paper „Countering hybrid Threats",* žiūrėta 2026 m. sausio 25 d., https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf.

[86] Rasmus Hindrén, *Hybrid threats and the EU's Strategic Compass*, (Helsinkis: European Centre of Excellence for Countering Hybrid Threats, 2021), 12, https://www.hybridcoe.fi/wp-content/uploads/2021/10/Hybrid_CoE_Working_Paper_12_Calibrating_the_compass_WEB.pdf.

4) svarbiausios infrastruktūros (energijos tinklų, transporto, kosmoso) apsaugos stiprinimas;

5) bendradarbiavimas su trečiosiomis šalimis;

6) finansavimo, skirto hibridinėms grėsmėms, užkardymas;

7) valstybių narių bendradarbiavimo stiprinimas su NATO.[87]

Aptartas komunikatas buvo vienas svarbiausių dokumentų, suteikęs bendrą grėsmių supratimą bei padėjęs pagrindus tolimesniam ES atsakui.

Kitas didelę reikšmė turintis dokumentas kovoje su hibridinėmis grėsmėmis yra 2018 m. birželio mėnesį, priimtas komunikatas **„Atsparumo didinimas ir kovos su hibridinėmis grėsmėmis pajėgumų plėtra"**[88], kuris yra ankščiau minėto „*Bendros sistemos, kovojant su hibridinėmis grėsmėmis*" komunikato užsibrėžtų tikslų ir veiksmų įgyvendinimo apžvalga, bei tolimesnių veiksmų planas. Komunikate kalbama apie besitęsiantį ES susidūrimą su valstybinių ir nevalstybinių subjektų hibridine veikla, kuri kelia didelę grėsmę valstybės narėms, taip pat pastebimas pastangų mažinti visuomenės pasitikėjimą valstybių institucijomis, destabilizuoti padėtį šalyse padidėjimas. Komunikate pabrėžtas poreikis glaudžiai bendradarbiauti su Šiaurės Atlanto sutarties organizacija (NATO), kitais tarptautiniais subjektais, taip pat stiprinti strateginės komunikacijos, kibernetinės veiklos ir kontražvalgybos sričių pajėgumus atpažinti hibridines grėsmes ir į jas atsakyti.[89]

Europos Sąjungai toliau vykdant aktyvią kovą su hibridinėmis grėsmėmis, 2022 metais buvo patvirtintas **„Strateginis saugumo ir gynybos kompasas"**. Šis dokumentas apibendrina ir apibrėžia ES veiklą saugumo ir gynybos srityje iki 2030 metų, jame taip pat pateikiamas veiksmų planas, strateginės aplinkos vertinimas, išryškinami bendri ES tikslai.[90] Planą sudaro keturios pagrindinės veikimo kryptys: a) bendradarbiavimas; b) apsauga; c) veikimas; d) investavimas. Bendradarbiavimo srityje numatyta stiprinti partnerystę su NATO, Jungtinėmis Tautomis, kitomis organizacijomis ir partneriais; vystyti dvišalį bendradarbiavimą su Kanada, Norvegija, Jungtine Karalyste, Japonija ir kitomis šalimis, gerinti dialogą ir bendradarbiavimą su Vakarų Balkanų šalimis, Afrikos, Azijos ir Lotyno Amerikos šalimis, kartu dalyvauti misijose ir operacijose.[91] Apsaugos srityje, bus siekiama stiprinti informacijos analizės žvalgybinius pajėgumus, vystyti ES

[87] European Commision, *Ibid.*

[88] Europos Komisija, *Atsparumo didinimas ir kovos su hibridinėmis grėsmėmis pajėgumų plėtra. Bendras komunikatas* (JOIN(2018) 16 final, 2018 m. birželio 13 d.), žiūrėta 2026 m. vasario 11 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52018JC0016.

[89] *Ibid.*

[90] „Lietuvos dalyvavimas ES bendroje saugumo ir gynybos politikoje (BSGP)", *Lietuvos Respublikos užsienio reikalų ministerija*, žiūrėta 2026 m. vasario 11 d., https://www.urm.lt/lietuvos-saugumo-politika/lietuvos-dalyvavimas-es-bendroje-saugumo-ir-gynybos-politikoje-bsgp/309.

[91] European Union External Action Service, „*A Strategic Compass for Security and Defence*", žiūrėta 2026 m. vasario 11 d., https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

priemonių rinkinį kovai su hibridinėmis grėsmėmis ir greitojo reagavimo komandas, panaudojant skirtingas priemones identifikuoti ir reaguoti į plataus spektro hibridines grėsmes, tobulinti kibernetinio saugumo įrankius, ES Kibernetinės gynybos politiką, ES Kosmoso strategiją saugumui ir gynybai, stiprinti ES vaidmenį jūrų saugumo zonoje.[92] Veikimo srityje, bus įkurta ES greitojo reagavimo grupė, kurią sudarys apie 5 tūkst. karių. Komanda bus skirta veikti ištikus įvairioms krizėms. Be kita ko, tikimasi būti pasiruošus išsiųsti 200 pilnai aprūpintų bendros saugumo ir gynybos politikos (angl. CSDP) ekspertų per 30 dienų nuo grėsmės atsiradimo, vykdyti reguliarias pratybas, padidinti kariuomenės mobilumą, pilnai išnaudoti Europos taikos priemones palaikant savo partnerius.[93] Investavimo srityje, valstybės narės įsipareigoja padidinti gynybos išlaidas, sustiprinti Europos gynybos technologijų ir pramonės bazę. Tuo tarpu ES iniciatyva, bus keičiamasi nuomonėmis dėl nacionalinių tikslų didinant išlaidas gynybai, jog tai atitiktų saugumo poreikius, valstybės narės bus skatinamos įsitraukti į bendrų pajėgumų vystymą ir kartu investuoti į naujos kartos galimybes veikti žemyne, jūroje ir ore, taip pat kibernetinėje erdvėje bei kosmose, sumažinti technologinį ir pramoninį priklausomumą nuo kitų šalių.[94]

Aptartame strateginiame kompase buvo pabrėžta ir būtinybė parengti **ES hibridinių priemonių rinkinį** (angl. Hybrid Toolbox), kuris *„[...] turėtų apimti esamas ir galimas naujas priemones ir tapti pagrindu koordinuotam atsakui į hibridines grėsmes, darančias poveikį ES ir jos valstybėms narėms. Priemonių rinkinys turėtų apimti prevencines, bendradarbiavimo, stabilizavimo, ribojamąsias ir atkūrimo priemones ir stiprinančiu solidarumą bei savitarpio pagalbą [...]*".[95] Atsižvelgiant į tai, 2022 metais, buvo įgyvendintas vienas iš ankščiau minėto kompaso tikslų ir sukurtas ES hibridinių priemonių rinkinys. Pagrindinis rinkinio tikslas, didinti ES ir jos valstybių narių atsparumą, stiprinti atgrasymą, taip pat suformuoti doktriną, kuri leistų aktyviai reaguoti ir atremti hibridines grėsmes. Rinkiniu taip pat norėta skatinti savitarpio pagalbą ir parodyti, kad hibridinė ataka prieš vieną, yra hibridinė ataka prieš visas valstybes nares.[96]

2024 m. Europos Vadovų Taryba priėmė susitarimą dėl 2024-2029 metų strateginės darbotvarkės, ES prioritetų ir strateginių gairių, kuriomis savo veikloje vadovaujasi visos ES institucijos. Darbotvarkėje nurodoma, kad ES stiprins savo atsparumą, pasiruošimą, krizių prevenciją ir reagavimo pajėgumus. Be kita ko, bus stiprinamas ir kolektyvinis atsakas į kibernetinį bei hibridinį karą, užsienio valstybių manipuliavimą ir grėsmes ypatingos svarbos infrastruktūrai.[97]

---

[92] *Ibid*.
[93] *Ibid.*
[94] *Ibid.*
[95] Europos Sąjungos Taryba, *Tarybos išvados dėl pagrindo koordinuotam ES atsakui į hibridines kompanijas*, žiūrėta 2026 m. vasario 11 d., https://data.consilium.europa.eu/doc/document/ST-10016-2022-INIT/lt/pdf.
[96] Kenneth Lasoen, „Realising the EU Hybrid Toolbox: opportunities and pitfalls", Clingendael, žiūrėta 2026 m. vasario 16 d., https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf.
[97]Europos Vadovų Taryba, „Strategic Agenda 2024–2029", žiūrėta 2026 m. vasario 16 d., https://www.consilium.europa.eu/media/yxrc05pz/sn02167en24_web.pdf.

Kitas svarbus strateginis dokumentas savisaugos ir atsparumo vystymui ES mastu, yra 2025 metų kovo mėnesį, Europos Komisijos patvirtinta **Europos Sąjungos parengties strategija**. Tai išsamus veiksmų planas, numatantis priemones sustiprinti visuomenės atsparumą, užtikrinti produktyvų atsaką į esamas grėsmes, suvienodinti grėsmių suvokimą. Strategijoje išskirtos pagrindinės grėsmės: stichinės nelaimės, žmogaus sukeltos nelaimės, hibridinės grėsmės, geopolitinės krizės. Hibridinių grėsmių tarpe išskirtos kibernetinės atakos, dezinformacijos kampanijos ir užsienio informacijos manipuliavimas ir kišimasis, ypatingai svarbios infrastruktūros sabotažas.[98] Taip pat iškelti septyni pagrindiniai strategijos tikslai: prognozavimo ir numatymo pajėgumų stiprinimas; gyvybiškai svarbių visuomenės funkcijų apsauga; gyventojų pasirengimo skatinimas; viešojo ir privačiojo sektorių bendradarbiavimo stiprinimas; civilinio ir karinio bendradarbiavimo stiprinimas; reagavimo į nelaimes koordinavimo centro stiprinimas; bendradarbiavimo su išorės partneriais stiprinimas.[99]

2025 metų balandžio mėnesį, buvo pristatytas dar vienas komunikatas **„ProtectEU“ - Europos vidaus saugumo strategija**. Komunikate teigiama, jog „*nebeaiški hibridinių grėsmių ir atviro karo perskyra*“.[100] Saugumo strategijoje, Europos Komisija įsipareigoja didinti operatyvinius, analitinius gebėjimus nustatyti ir švelninti kylančias hibridines grėsmes, taip pat numatoma didinti atsparumą hibridinėms grėsmėms, gerinant ypatingos svarbos infrastruktūros apsaugą, stiprinant kibernetinį saugumą kovojant su internetinėmis grėsmėms bei stiprinti transporto mazgų ir uostų saugumą. Atsižvelgiant į prieš kelis metus kilusią pabėgelių krizę Europoje, akcentuojamas ir išorės sienų saugomo stiprinimas, Šengeno informacinės sistemos tobulinimas.[101] Įgyvendinant saugumo strategijoje užsibrėžtus tikslus dėl hibridinių grėsmių, 2026 metų vasarį, ES komisija pristatė naują kovos su terorizmu darbotvarkę. Darbotvarkėje išskirtos šešios pagrindinės sritys: grėsmių numatymas, radikalizacijos prevencija, žmonių apsauga internete ir fizinėje aplinkoje, reagavimas į grėsmės ir išpuolius, bendradarbiavimas su partneriais.[102] Kitos Europos vidaus saugumo strategijoje numatytos priemonės, baigiamojo darbo rengimo metu, vis dar yra įgyvendinimo stadijoje ir konkrečių rezultatų pasiekta nėra.

Vis dėl to, ES vystydama ir įgyvendindama įvairias saugumo iniciatyvas, strategijas dėl hibridinių grėsmių, susiduria su sunkumais. Visų pirma, nors daugelis hibridinių atakų technikų

[98] Europos Sąjunga, „EU Preparedness Union Strategy”, Europos Sąjungos leidinių biuras, žiūrėta 2026 m. vasario 16 d., https://commission.europa.eu/topics/preparedness_en.
[99] „Europos Sąjungos parengties strategija: koordinuotas atsakas į šių dienų grėsmes“, Lietuvos Respublikos vidaus reikalų ministerija, žiūrėta 2026 m. vasario 16 d., https://vrm.lrv.lt/lt/naujienos/europos-sajungos-parengties-strategija-koordinuotas-atsakas-i-siu-dienu-gresmes/.
[100] *„ProtectEU“ – Europos vidaus saugumo strategija*“, Europos Komisija (COM(2025) 148 final), žiūrėta 2026 m. vasario 16 d., https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A52025DC0148.
[101] Ibid.
[102] „„ProtectEU“. Komisija pristato naują kovos su terorizmu darbotvarkę“, Europos Komisija, žiūrėta 2026 m. gegužės 4 d., https://ec.europa.eu/commission/presscorner/detail/lt/ip_26_423.

nėra naujos ir jau gerokai seniau buvo naudojamos prieš geopolitinius varžovus ar kitus subjektus, staigūs technologiniai pasikeitimai ir globalizacija, sudarė sąlygas hibridinėms grėsmėms įgyti dar didesnį pagreitį, mąstą ir intensyvumą.[103] Visų antra, hibridinės grėsmės suteikia pranašumą tiek valstybiniams, tiek ir nevalstybiniams subjektams. Nevalstybiniai subjektai šiuos metodus naudoja, dėl savo turimų nedidelių pajėgumų, palyginus su valstybių ar aljansų turimais konvenciniais pajėgumais. Valstybiniams subjektams tokie metodai palankūs, nes neperžengiama oficialaus karo riba, taip pat dėl kylančio dviprasmiškumo yra sunkiai priskiriami konkrečiam vykdytojui. Abiem atvejais, iš vyriausybių yra reikalaujama kūrybiškumo ir efektyvių sprendimų, kurie derėtų su demokratinėmis vertybėmis ir būtų išvengtą įvykių eskalacijos.[104] Trečia, dėl plačios hibridinių grėsmių apimties jas sunku prognozuoti, todėl valstybių prioritetas turėtų būti lanksčių ir lengvai pritaikomų metodų nenumatytiems atvejams, kūrimas.[105]

Apibendrinant galime teigti, kad ankščiau taikytos saugumo priemonės ir reagavimo algoritmai į hibridines grėsmes ES šalyse tapo neveiksmingi, todėl yra būtinas esamų priemonių atnaujinimas ir naujų kūrimas. Kaip reakciją į tai, Europos Sąjunga pradėjo kryptingą ir nuoseklų darbą hibridinių grėsmių atsparumo, prevencijos ir kovos srityje: priimtas ,,Bendros sistemos, kovojant su hibridinėmis grėsmėmis" komunikatas, ES hibridinių priemonių rinkinys, ,,Atsparumo didinimo ir kovos su hibridinėmis grėsmėmis pajėgumų plėtros" komunikatas, „Strateginis saugumo ir gynybos kompasas", Europos Sąjungos parengties strategija, „ProtectEU" - Europos vidaus saugumo strategija, Europos Vadovų Tarybos priimtas susitarimas dėl 2024-2029 metų strateginės darbotvarkės. Minėtos Strategijos, komunikatai ir kiti dokumentai rodo, jog hibridinių grėsmių keliami pavojai yra realūs ir toliau išlieka prioritetiniu Europos Sąjungos klausimu saugumo srityje. Kovoje su hibridinėmis grėsmėmis, ES akcentuoja kibernetinį, ypatingos svarbos infrastruktūros saugumą, valstybių narių tarpusavio bendradarbiavimą, prevencinių ir atsakomųjų veiksmų koordinuotumą, bendradarbiavimą su sąjungininkais, tarp jų ir NATO.

2.2 NATO ir ES strateginė sąveika kovojant su hibridinėmis grėsmėmis

Hibridinių grėsmių kompleksiškumas, neapibrėžtumas ir daugybės skirtingų sričių apėmimas savaime reikalauja didelio atsparumo, teisėkūros, strateginės komunikacijos ir kitų saugumo priemonių arsenalo. Dėl įvardintų priežasčių, stipriam ir efektyviam atsakui į tokio tipo grėsmes, vienos valstybės ar organizacijos pastangų neužtenka, todėl šiame kontekste NATO ir Europos Sąjungos partnerystė įgyja esminę reikšmę. Maria Malksoo įsitikinimu, ES ir NATO savo veikloje remiasi ir vadovaujasi tomis pačiomis specifinėmis vertybėmis. Autorė taip pat priduria,

[103] Lisboa, *supra note*, 7: 3.
[104] *Ibid.*
[105] *Ibid.*

kad hibridinių grėsmių atlaikymas yra tiesiogiai susijęs su ES ir NATO išlikimu.[106] NATO tinklapyje 2026 metų sausį parengtame pranešime nurodoma, kad *„NATO negali įveikti hibridinių grėsmių viena. Bendradarbiavimas su partneriais yra esminis. Aljansas ir toliau stiprins bendradarbiavimą su partneriais, tarp jų ir Europos Sąjunga, didinant atsparumą ir kovojant su hibridinėmis grėsmėmis."*[107]

Europos Sąjungos ir NATO bendradarbiavimo pradžią hibridinių grėsmių srityje žymi 2016 metais Varšuvoje, Europos Tarybos, Europos Komisijos prezidentų ir Šiaurės Atlanto sutarties organizacijos generalinio sekretoriaus pasirašyta **„Jungtinė deklaracija"**, kuri suteikė nauja turinį ir impulsą strateginei partnerystei. Deklaracijoje pažymimas būtinumas gerinti pajėgumus hibridinių grėsmių klausimu, o būtent didinant atsparumą, dirbant kartu analizės, prevencijos, informacijos dalijimosi, strateginės komunikacijos srityse, taip pat dalyvaujant koordinuotose pratybose dėl hibridinių atakų.[108]

NATO viršūnių susitikime Briuselyje, 2018 metais buvo paskelbtas ***kovos su hibridinėmis grėsmėmis paramos komandos*** įkūrimas, kuri pagal sąjungininko išreikštą prašymą bus pasiruošusi suteikti pritaikytą ir tikslinę pagalbą pasiruošiant ir reaguojant į hibridines veiklas.[109] Paramos komandos praktinė nauda 2026 metų vasarį, Lietuvai pateikus prašymą buvo išbandyta ir mūsų šalyje. Susitikimo su įvairių institucijų atstovais, buvo aptarta situacija ir taikomos reagavimo priemonės. Po apsilankymo, paramos grupė turės pateikti rekomendacijas dėl oro gynybos nuo dronų stiprinimo, kontrabandai naudojamų oro balionų ir kaip kovoti su informacinėmis grėsmėmis.[110] Tai jau ne pirmas paramos komandos apsilankymas Lietuvoje - 2021 metais ji buvo atvykusi į Lietuvą dėl ištikusios migrantų krizės prie Baltarusijos sienos.

2022 m. birželio 29 dieną Madride vykusiame NATO viršūnių susitikime patvirtinta ateinančio dešimtmečio **„NATO 2022 Strateginė Koncepcija"**. Joje Europos Sąjunga yra apibūdinama, kaip unikali ir esminė, tomis pačiomis vertybėmis besidalinanti labai svarbi NATO partnerė. Strategijoje įsipareigojama investuoti į pasiruošimą, palaikyti partnerius, tarp jų ir ES, valstybinių ir nevalstybinių subjektų keliamoms hibridinėms grėsmėms atremti. Svarbu paminėti, kad strategijoje taip pat nurodoma, kad hibridinės operacijos prieš sąjungininkus, gali peraugti į

---

[106] Maria Mälksoo, „Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO", European Security 27, 3 (2018): 12, https://doi.org/10.1080/09662839.2018.1497984.

[107] „Countering hybrid threats", NATO, žiūrėta 2026 m. vasario 20 d., https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.

[108] „Joint declaration", NATO, žiūrėta 2026 m. vasario 20 d., https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/joint-declaration.

[109] „Brussels Summit Declaration", NATO, žiūrėta 2026 m. vasario 20 d., https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2018/07/11/brussels-summit-declaration.

[110] „Lietuvoje lankėsi NATO kovos su hibridinėmis grėsmėmis paramos komanda", Lietuvos Respublikos užsienio reikalų ministerija, žiūrėta 2026 m. vasario 20 d., https://www.urm.lt/naujienos/141/lietuvoje-lankesi-nato-kovos-su-hibridinemis-gresmemis-paramos-komanda:45568.

ginkluotą užpuolimą ir sudaryti precedentą aljansui aktyvuoti 5 Šiaurės Atlanto sutarties straipsnį.[111]

2023 metų sausio mėnesį buvo pasirašyta dar viena, **„Jungtinė ES – NATO bendradarbiavimo deklaracija"**. Joje dar kartą pabrėžiama Europos Sąjungos ir NATO strateginės partnerystės svarba, dalijimasis bendromis vertybėmis ir pareiga ginti Euro-Atlantinę zoną. Dokumente įvardijama, kad partnerystės laikotarpiu buvo pasiekti apčiuopiami rezultatai hibridinių, kibernetinių grėsmių srityje, taip pat kovoje su terorizmu, gynybos pramonėje, pajėgumų stiprinime. Deklaracija įsipareigojama ir toliau plėtoti NATO ir ES partnerystę, konsultuotis su valstybėmis narėmis, stiprinti kritinės infrastruktūros apsaugą, spręsti iškilusias problemas susijusias su trikdančiomis technologijomis, užsienio informacine manipuliacija ir kišimusi bei kt.[112]

Europos Sąjungai ir NATO toliau vienijant savo jėgas, bei reaguojant į „Nord Stream" dujotiekių sabotažus ir kitas hibridines atakas, 2023 m. kovo 16 d., buvo įsteigta **EU - NATO darbo grupė** (angl. Task Force), skirta kritinės infrastruktūros atsparumo ir saugumo stiprinimui. Europos Komisijos prezidentė Ursula von der Leyen, darbo grupės pristatymo metu nurodė, kad „*EU ir NATO vyresnieji ekspertai dirbs kartu, kad nustatytų grėsmes mūsų kritinei infrastruktūrai ir parengtų atsaką*".[113] Darbo grupėje bus dalijamasi gerąja praktika, vystomi esminiai atsparumo principai. Jos veikla apims keturis sektorius: energetikos, transporto, kosmoso ir skaitmeninės infrastruktūros.[114]

Išanalizavus ES komunikatus ir strategijas, galime teigti, jog hibridinių grėsmių poveikis įvairiems valstybės sektoriams rodo, kad nė viena valstybė savarankiškai negali užtikrinti efektyvaus atsako į tokio pobūdžio grėsmes. Dėl šios priežasties NATO ir ES partnerystė hibridinių grėsmių kontekste pereina nuo tradicinio politinio bendradarbiavimo modelio į visapusišką strateginio saugumo sistemą: NATO užtikrina kolektyvinę gynybą, atgrasymą ir reagavimą, o Europos Sąjunga vykdo teisėkūros, reguliavimo ir vidaus atsparumo stiprinimo priemones. Šių dviejų organizacijų bendradarbiavimas nuosekliai stiprėja ir įgauna vis didesnę praktinę reikšmę per bendras deklaracijas, koordinuotas pratybas, informacijos mainus, kritinės infrastruktūros apsaugos iniciatyvas bei paramos mechanizmus valstybėms narėms.

---

[111] „NATO 2022 Strategic Concept", NATO, žiūrėta 2026 m. vasario 18 d., https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept.

[112] „Joint Declaration on EU-NATO Cooperation", NATO, žiūrėta 2026 m. vasario 20 d., https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/01/10/joint-declaration-on-eu-nato-cooperation.

[113] „Launch of the EU-NATO Task Force", Europos Komisija, žiūrėta 2026 m. vasario 18 d., https://ec.europa.eu/commission/presscorner/detail/ga/statement_23_1705.

[114] *Ibid.*

2.3 Lietuvos nacionalinio saugumo strategijos kryptys ir teisinis reguliavimas kovoje su hibridinėmis grėsmėmis

Lietuvos nacionalinio saugumo užtikrinimas yra grindžiamas aiškiai apibrėžta strategine ir teisine sistema, kurios pagrindinis tikslas užtikrinti valstybės nepriklausomybę, teritorinį vientisumą, demokratinę santvarką bei visuomenės saugumą. Šiandieninio pasaulio saugumo kontekste hibridinės grėsmės įgauna vis didesnę reikšmę. Jomis siekiama paveikti valstybę ir jos gyventojus laviruojant tarp karinio konflikto ribos. Reaguodama į tai, Lietuvos nacionalinio saugumo sistema priversta vis daugiau dėmesio skirti hibridinių grėsmių atsparumui ir gynybai.

Vienas iš pagrindinių Lietuvos nacionalinį saugumą reglamentuojančių teisės aktų yra Lietuvos Respublikos (toliau LR) nacionalinio saugumo pagrindų įstatymas, priimtas dar 1996 metais. Šiuo įstatymu yra įtvirtinami svarbiausi nacionalinio saugumo principai, reglamentuojama nacionalinio saugumo sistema, pagrindinės vidaus ir užsienio politikos kryptys, nacionalinį saugumą užtikrinančių institucijų veikla.[115] Nacionalinį saugumą Lietuvoje taip pat reglamentuoja ir kiti nacionaliniai teisės aktai: LR Konstitucija, LR nacionalinio saugumo strategija, taip pat ir tarptautiniai teisės aktai: Jungtinių Tautų Chartija, Europos saugumo ir bendradarbiavimo organizacijos dokumentai, įvairios daugiašalės ir dvišalės tarptautinės sutartys, o visi su Lietuvos nacionalinio saugumo strategiją susiję veiksmai yra derinami su Europos Sąjungos bendros saugumo ir gynybos politikos strateginiais tikslais.[116] Visgi, LR nacionalinio saugumo pagrindų įstatyme, hibridinės grėsmės minimos nėra. Tačiau galima teigti, kad šiuo įstatymu yra sukuriama bendra nacionalinio saugumo užtikrinimo sistema, o konkretesnis grėsmių identifikavimas ir jų turinys yra atskleidžiamas vėlesniuose teisiniuose dokumentuose. Tą patvirtina Lietuvos nacionalinio saugumo strategija, priimta 2021 metais, kuri yra „*svarbiausių saugios valstybės raidą apibrėžiančių nuostatų visuma. Remiantis Lietuvos Respublikos Konstitucijoje įtvirtintomis vertybėmis, Nacionalinio saugumo strategijoje yra nustatomi esminiai nacionalinio saugumo interesai, pagrindiniai rizikos veiksniai, pavojai ir grėsmės šiems interesams, įtvirtinami valstybės nacionalinio saugumo sistemos plėtros, užsienio, gynybos ir vidaus politikos prioritetai, ilgojo laikotarpio uždaviniai valstybės saugumo būklei užtikrinti.*”[117] Strategijoje nurodoma, kad „*grėsmių kompleksiškumas pasižymi nykstančiomis skirtimis tarp karo ir taikos, išorinių ir vidinių, karinių ir nekarinių grėsmių, valstybinių ir nevalstybinių grėsmių šaltinių. Tai lemia didesnį hibridinių grėsmių iššūkį euroatlantinei bendruomenei, taigi ir Lietuvos Respublikai. Nekarinės,*

[115] „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, TAR, žiūrėta 2026 m. vasario 26 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.A0BAB27D768C/hlQneKjoWb.

[116] Asta Petrauskaitė, Rasa Kazlauskaitė-Markelienė ir Rasa Gedminienė, *Šalies saugumas ir gynyba: metodinė medžiaga Lietuvos bendrojo lavinimo mokyklų mokytojams* (Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2016), 9, https://biblioteka.lka.lt/data/Leidiniai/sisteminis_katalogas/Informaciniai-reprezentaciniai/2016-salies saugumas ir gynyba-metodine.pdf.

[117] „Nacionalinis saugumas”, Lietuvos Respublikos krašto apsaugos ministerija, žiūrėta 2026 m. vasario 26 d., https://kam.lt/duk/nacionalinio-saugumo-strategija/.

ardomosios veiklos priemonės vis dažniau naudojamos siekiant paveikti euroatlantinės bendruomenės valstybių saugumo interesus."[118] Įstatyme, tarp nacionalinio saugumo politikos prioritetų ir uždavinių, valstybės ir visuomenės atsparumo srityje, buvo iškelti tokie su hibridinėmis grėsmėmis susiję uždaviniai, kaip: viešąjį saugumą užtikrinančių institucijų gebėjimų ir pajėgumų vystymas veikti krizių, ekstremaliųjų situacijų metu arba atremti hibridines grėsmes, užtikrinti valstybinės reikšmės objektų, turto ar įrenginių fizinę apsaugą, taip pat stiprinti civilinės saugos sistemos pajėgumus, bendradarbiavimą su NATO ir ES.[119]

Valstybei stiprinant pasiruošimą atremti hibridinės grėsmes, 2022 m. gruodžio 8 d. Seime buvo priimtas naujas **Krizių valdymo ir civilinės saugos įstatymas**, kuriuo į valstybės krizių valdymo ir civilinės saugos sistemą buvo įtrauktas naujas subjektas – Nacionalinis krizių valdymo centras (toliau NKVC). Tai atskiras ir išskirtinis Vyriausybės kanceliarijos padalinys, tapęs svarbiausia institucija valdant krizes ir ekstremalias situacijas šalyje.[120] NKVC savo darbą pradėjo 2023 m. Sausio 1 d. Centras visą parą vykdo grėsmių analizę ir jų vertinimą, atlieka iškilusios krizės ar valstybės lygio ekstremaliosios situacijos prevenciją, valdymo planavimą ir organizavimą, strateginės komunikacijos koordinavimą. Be kita ko, šis padalinys yra atsakingas ir už valstybės ar tarptautiniu lygmeniu organizuojamas krizių valdymo pratybas, taip pat bendradarbiavimą su tarptautiniais partneriais krizių valdymo srityje. Tai pagrindinis sprendimų planavimo padalinys dėl hibridinių grėsmių keliamų pavojų, kai jos apima kelių savivaldybių ekstremaliosios situacijos mastą ar perauga į krizę.[121]

Įgyvendinant Lietuvos Nacionalinio saugumo strategijoje formuluojamą uždavinį vystyti viešąjį saugumą užtikrinančių institucijų gebėjimus ir pajėgumus atremti hibridines grėsmes, Vidaus reikalų ministerija parengė kompleksines VRM sistemos atsparumo hibridinėms grėsmėms gaires. Gairėmis siekiama stiprinti VRM statutinių tarnybų bendrą pasiruošimą reaguoti į hibridines grėsmes.[122] Pirmuoju gairių įgyvendinimo pavyzdžiu tapo 2023 m. surengtos bendros Lietuvos policijos antiteroristinių operacijų rinktinės „Aras", Valstybės sienos apsaugos tarnybos Specialiosios paskirties skyriaus, Viešojo saugumo tarnybos ir Operatyvaus reagavimo

[118] „Dėl Nacionalinio saugumo strategijos patvirtinimo", *supra note*, 55.
[119] *Ibid*.
[120] „Dėl Lietuvos Respublikos Vyriausybės kanclerio 2023 m. sausio 19 d. įsakymo Nr. V-15 „Dėl Lietuvos Respublikos Vyriausybės kanceliarijos 2023–2025 metų strateginio veiklos plano patvirtinimo" pakeitimo", Lietuvos Respublikos Vyriausybė, žiūrėta 2026 m. vasario 27 d., https://lrv.lt/media/viesa/saugykla/2023/12/9KvAXF0cYHk.pdf.
[121] Matonytė, Gajauskaitė ir Denisenko, *supra note*, *19:* 41.
[122] „Hibridinėms grėsmėms – vieningas VRM tarnybų atsakas", Lietuvos Respublikos vidaus reikalų ministerija, žiūrėta 2026 m. vasario 27 d., https://vrm.lrv.lt/lt/naujienos/hibridinems-gresmems-vieningas-vrm-tarnybu-atsakas.

kontratakos komandos (ORKA) pareigūnų pratybos „Sąveika-2023“. Pratybos buvo orientuotos į kritinės infrastruktūros apsaugą, kuri yra vienas pagrindinių priešo taikinių.[123]

Hibridinių grėsmių pobūdis lemia tai, kad valstybė gali būti pažeidžiama ne tik kariniame, bet ir kritinės infrastruktūros, kibernetinio saugumo ar energetikos sektoriuose. Dėl šios priežasties kritinės infrastruktūros apsauga, civilinės saugos stiprinimas tampa vienos svarbiausių nacionalinio saugumo politikos įgyvendinimo krypčių. Vis dėlto vien tik strateginių nuostatų įtvirtinimas savaime neužtikrina veiksmingo atsako į hibridines grėsmes. Tam reikalingos konkrečios teisinio reguliavimo priemonės, bei jų įgyvendinimas. Dėl to, 2024 metų liepos 18 d. reaguojant į hibridines grėsmes, buvo priimtas nutarimas **„Dėl civilinės saugos stiprinimo ir plėtros programos patvirtinimo”**[124], kuriuo buvo patvirtinta civilinės saugos stiprinimo ir plėtros programa, skirta valstybės saugumo stiprinimui, siekiant įgyvendinti, anksčiau minėtą 2021 metų Nacionalinio saugumo strategiją. Būtinybė kurti ir tobulinti gyventojų saugumą Lietuvoje didžiąją dalimi lemia geopolitinė situacija ir geografinė šalies padėtis. Programos II skyriaus 8.2 punkte nurodoma, kad *„Rusijos Federacijos ir Baltarusijos Respublikos agresija kaimyninių valstybių atžvilgiu pablogino saugumo situaciją regione ir pasaulyje - padidėjo karinių ir hibridinių grėsmių rizika. Esant tokiai saugumo padėčiai neatmestinas priešiškų valstybių bandymas instrumentalizuoti ekstremaliąsias situacijas, pavyzdžiui, dirbtinai jas sukeliant ar bandant jas sukelti vienu metu geografiškai plačiai, siekiant sutrikdyti civilinės saugos pajėgų veiklą ir reagavimą ar gyvybiškai svarbių paslaugų teikimą gyventojams - elektros energijos, dujų, šilumos ar vandens tiekimą”.*[125] Programoje išskirtos septynios prioritetinės veiksmų grupės, o priemonėms įgyvendinti skirtas 2024-2030 metų laikotarpis.

3 lentelė. Civilinės saugos stiprinimo kryptys ir priemonės

CIVILINĖS SAUGOS STIPRINIMO KRYPTYS	PRIEMONĖS STIPRINTI CIVILINĘ SAUGĄ
Priedangų infrastruktūros plėtra	1. Didinamas priedangų skaičius, kad jose ne mažiau kaip 50 proc. gyventojų turėtų galimybę pasislėpti.
Perspėjimo sistemų tobulinimas, gyventojų informavimo tobulinimas	1. Tobulinama gyventojų perspėjimo sistema, įtraukiant informacijos transliavimą per televiziją, radiją, internetą ir socialinius tinklus. 2. Sukurti mobiliąją programėlę „LT72”. 3. Užtikrinti gyventojų švietimą civilinės saugos klausimais, didinti visuomenės

[123] „Vilniaus rajone – taktinės pratybos „Sąveika 2023“ (foto)“, Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos, žiūrėta 2026 m. vasario 27 d., https://vsat.lrv.lt/lt/naujienos/vilniaus-rajone-taktines-pratybos-saveika-2023-foto/.
[124] „Nutarimas *„Dėl civilinės saugos stiprinimo ir plėtros programos patvirtinimo“,* TAR, žiūrėta 2026 m. kovo 23 d., https://e-tar.lt/portal/lt/legalAct/74b9f360459211efbdaea558de59136c.
[125] *Ibid.*

	pasirengimą hibridinėms ir karinėms grėsmėms.
Krizių valdymo ir civilinės saugos sistemos subjektų parengties ir atsparumo didinimas	1. Stiprinami gyventojų evakavimo pajėgumai. 2. Komendantūrų įsteigimas.
Sveikatos apsaugos sistemos stiprinimas	1. Didinamas sveikatos priežiūros įstaigų infrastruktūros atsparumas, pritaikymas veikti krizių ir karo metu. 2. Specialistų mokymai, kompetencijų tobulinimas. 3. Medicininių atsargų kaupimas ir palaikymas Lietuvoje.
Civilinės saugos pagalbos komandų formavimas	1. Sukurtos visą parą veikiančios PAGD greitojo reagavimo komandos.
Pasirengimo cheminėms, biologinėms ir branduolinėms grėsmėms stiprinimas	1. Stiprininamas civilinės saugos pajėgų ir kitų subjektų pasirengimas reaguoti į branduolines ir radiologines avarijas, cheminių, biologinių ir radioktyviųjų medžiagų aptikimas, identifikavimas ir stebėsena, pajėgų aprūpinimas reikiama technika, įranga bei priemonėmis. 2. Rengiamos valstybės lygio civilinės saugos pratybos, dalyvaujama užsienio šalių organizuojamose pratybose, stiprinamas bendradarbiavimas su užsienio valstybių laboratorijomis. 3. Didinamos investicijos.
Civilinės saugos mokymo pajėgumų stiprinimas	1. Didinami Ugniagesių gelbėtojų mokyklos civilinės saugos mokymo pajėgumai, investuojama į mokymų bazės plėtrą, žmogiškuosius išteklius, kompetencijų kėlimą. 2. Ypatingas dėmesys bus skiriamas ne tik teorinių žinių teikimui, bet ir praktinių įgūdžių formavimui, į mokymo procesą įtraukiant ekspertus, ypač Lietuvos šaulių sąjungą.

Šaltinis: Sudaryta darbo autoriaus, remiantis *„2024 m. liepos 18 d. Nr. XIV-2946 Nutarimu dėl Civilinės saugos stiprinimo ir plėtros programos patvirtinimo“*[126]

Atkreiptinas dėmesys, kad nacionalinio saugumo strategijos ir politikos pakeitimai, turi būti atliekami reguliariai, atsižvelgiant į geopolitinę situaciją, gyvenimo laikmetį ir kitus veiksnius, tačiau ne rečiau kaip kas penkerius metus.[127] Baigiamojo darbo rengimo metu, atnaujinta 2026 metų Lietuvos nacionalinė saugumo strategija dar nėra priimta, tačiau 2026 metų vasario mėnesį, Nacionalinio saugumo strategijos projektui pritarė LR Ministrų kabinetas, kuris buvo perduotas svarstyti LR Seimui pavasario sesijoje. Parengtame projekte, įtvirtinamas prioritetas visapusiškos

[126] *Ibid.*
[127] Aušra Bertašienė, „Lietuvos nacionalinio saugumo rizikos veiksniai ir jų valdymas“ (magistro baigiamasis darbas, Klaipėdos universitetas, 2025), 19, https://portalcris.ku.lt/server/api/core/bitstreams/7d235b4f-b380-4f35-9d6f-54b026ae89cb/content.

valstybės gynybos, jos finansavimui, visuomenės pasirengimo krizėms ir sąjungininkų buvimui.[128] Atnaujintame nacionalinio saugumo politikos įgyvendinime, pagrindinis dėmesys bus skiriamas civilinei gynybai, gynybos pramonei, gynybos finansavimui, transatlantiniams ryšiams, kritinės infrastruktūros apsaugai, karinių pajėgų vystymui ir žvalgybos institucijų stiprinimui. Kritinės infrastruktūros apsaugos srityje, Lietuva sieks didinti saugumą ir atsparumą stiprinant šalies energetinį savarankiškumą, apsaugą nuo hibridinių grėsmių, kibernetinį saugumą ir bendradarbiavimą su sąjungininkais.[129]

Teisėkūros pakeitimai ne vienintelė naudojama priemonė stiprinanti šalies nacionalinį saugumą ir civilinės saugos sistemos veiksmingumą. 2026 metais valstybinė priešgaisrinė gelbėjimo tarnyba nuosekliai planuoja ir rengia pratybas, orientuotas į realiai galinčias kilti grėsmės - pramonines avarijas ar kitus hibridinius incidentus. Šių metų balandžio mėnesi pratybos buvo surengtos AB „Achema“ teritorijoje, kurioje imituota dronų ataka ir dėl jos kilęs gaisras. Pratybose dalyvavo apie 250 pareigūnų, kitų specialistų. Stiprinant gyventojų apsaugą ir jų pasirengimą veikti, bendradarbiaujant su Lietuvos Raudonojo Kryžiaus atstovais bus surengtos evakavimo pratybos, o kartu su savivaldybėmis bus organizuojamos bendros civilinės saugos pratybos.[130]

Didinant šalies gyventojų atsparumą, aktyvių veiksmų imasi ir LR Krašto apsaugos ministerija, kuri akcentuoja pilietinio pasipriešinimo rengimo svarbą ir piliečių žinias hibridinių grėsmių srityje: *„pagrindinė problema, susijusi su hibridiniais veiksmais, yra tai, kad piliečiai, neturintys pakankamai žinių, dažniausiai jų neatpažįsta - taip jie yra išnaudojami priešo hibridinių veiksmų schemose. Norint duoti tinkamą atkirtį priešo paruoštiems hibridiniams veiksmams yra būtina didinti visų Lietuvos piliečių žinias, kaip atpažinti hibridines grėsme ir taip didinti visos šalies atsparumą“*.[131] Organizuojamuose mokymuose mokoma pilietinio pasipriešinimo modulio, skirto būtent atsparumui hibridinėms grėsmėms stiprinti, jas atpažinti, taip pat prevencijai ir atsakui į jas valdyti. Ministerijos duomenimis, 2025 m. I ketvirtį, organizuojamus pilietinio pasipriešinimo mokymus išklausė 79 tūkst. asmenų, iš kurių 381 asmuo išklausė mokymus susijusius būtent su atsparumu hibridinėms grėsmėms.[132]

---

[128] „Ministrų kabinetas pritarė atnaujintam Nacionalinės saugumo strategijos projektui“, Lietuvos Respublikos Vyriausybė, žiūrėta 2026 m. vasario 25 d., https://lrv.lt/lt/naujienos/ministru-kabinetas-pritare-atnaujintam-nacionalines-saugumo-strategijos-projektui-myyf.

[129] *Ibid*.

[130] „Nelaimių nelaukiama: valstybinė priešgaisrinė gelbėjimo tarnyba stiprina pasirengimą realioms grėsmėms“, Priešgaisrinės apsaugos ir gelbėjimo tarnybos departamentas prie vidaus reikalų ministerijos, žiūrėta balandžio 8 d., https://pagd.lrv.lt/lt/naujienos/nelaimiu-nelaukiama-valstybine-priesgaisrine-gelbejimo-tarnyba-stiprina-pasirengima-realioms-gresmems-9Xr/.

[131] „Visuomenės pasirengimas visuotinei gynybai“, Lietuvos Respublikos Krašto apsaugos ministerija, žiūrėta 2026 m. vasario 25 d., https://kam.lt/visuomenes-pasirengimas-visuotinei-gynybai/.

[132] *Ibid*.

Stiprinant visuomenės pasirengimą ir jos didinant informuotumą civilinės saugos srityje, VRM iniciatyva, buvo sukurta mobilioji programėlė **LT72**. Programėlė skirta ugdyti savisaugos kultūrą, padėti gyventojams pasiruošti ekstremaliosioms situacijoms, pradedant nuo stichinių nelaimių, branduolinių avarijų, baigiant galimomis karinėmis grėsmėmis. Joje pateikiama informacija apie kolektyvines slėptuves, priedangas, gyventojų evakuacijos punktus.[133]

Regioninio saugumo stiprinimo kontekste, Lietuva, Latvija ir Lenkija 2026 m. vasario 25 d. pasirašė bendrą deklaraciją dėl sustiprinto bendradarbiavimo užtikrinant išorės sienų saugumą ir atsakant į hibridines grėsmes. Deklaracija numatoma stiprinti išorinių sienų saugumą nuo hibridinių grėsmių, migracijos, kontrabandos ar kitų atakų jūroje, sausumoje ir oro erdvėje. Šalys sieks veikti trimis kryptimis – pasirengimo, bendrų veiksmų ir atsako, o būtent dalintis informacija apie Rusijos ir Baltarusijos vykdomas hibridines atakas, bendradarbiauti nustatant už hibridinius veiksmus atsakingus subjektus, koordinuoti efektyvų atsaką.[134]

Apibendrinant galime teigti, jog Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, Lietuvos nacionalinio saugumo strategija yra pagrindiniai teisės aktai, apibrėžiantys nacionalinio saugumo suvokimą Lietuvoje, nustatantys pagrindinius interesus, prioritetus ir uždavinius, šalies nacionalinio saugumo srityje. Strategijoje pažymimas grėsmių kompleksiškumas bei hibridinių grėsmių keliami iššūkiai tiek Lietuvai, tiek ir NATO šalims. Dėl hibridinių grėsmių daugialypiškumo, buvusių priemonių nebeužtenka, todėl valstybė ir institucijos pereina nuo prevencijos, prie visuotinio saugumo ir gynybos stiprinimo. Įgyvendinant nacionalinio saugumo strategijos tikslus, valstybė imasi aktyvių priemonių kovojant su iškilusiomis hibridinėmis grėsmėmis: nuosekliai stiprinama civilinė sauga, įkurtas Nacionalinis krizių valdymo centras, gyventojai yra šviečiami hibridinių grėsmių ir pilietinio pasipriešinimo srityje, organizuojamos bendros valstybinių institucijų pratybos kritinės infrastruktūros apsaugos srityje.

[133] „LT72 – pasirengimo ekstremaliosioms situacijoms programėlė“, Lietuvos Respublikos Vidaus reikalų ministerija, žiūrėta 2026 m. balandžio 8 d., https://vrm.lrv.lt/lt/pasirengimo-ekstremaliosioms-situacijoms-programele-lt72/.
[134] „Lietuvos, Latvijos ir Lenkijos Premjerai paskelbė bendrą deklaraciją dėl išorinių sienų apsaugos stiprinimo ir atsako į hibridines grėsmes“, Lietuvos Respublikos Vyriausybė, žiūrėta 2026 m. vasario 27 d., https://lrv.lt/lt/naujienos/lietuvos-lenkijos-ir-latvijos-premjerai-paskelbe-bendra-deklaracija-del-isoriniu-sienu-apsaugos-stiprinimo-ir-atsako-i-hibridines-gresmes-7aaX/.

3. HIBRIDINIŲ GRĖSMIŲ ĮTAKA LIETUVOS NACIONALINIAM SAUGUMUI

Ankstesnėse magistro baigiamojo darbo dalyse buvo nustatyta, kad Lietuva susiduria su priešiškai nusiteikusių valstybių, ypač Rusijos vykdomomis hibridinėmis atakomis. 2026 metų Valstybės saugumo departamento parengtame Grėsmių nacionaliniam saugumui vertinime nurodoma, kad *„Lietuvai priešiški kaimyniniai režimai naudoja nekonvencines priemones, kurių tikslas – paveikti mūsų piliečių protus, kurti nesaugumo atmosferą ir versti mus priimti šiems režimams naudingus sprendimus. Cigarečių gabenimas oro balionais, keliantis grėsmę civilinei aviacijai, ar Lietuvos piliečių politiškai motyvuoti sulaikymai yra Baltarusijos režimo naudojamos spaudimo ir terorizavimo priemonės, kuriomis siekiama režimo tarptautinio pripažinimo ir šaliai taikomų ribojimų mažinimo.“*[135] Paminėtina, kad priešiškų subjektų taikinyje yra ne tik fizinė tačiau ir kibernetinė erdvė. Dėl ribotos baigiamojo darbo apimties, žemiau bus analizuojami tik meteorologinių balionų ir kibernetinių išpuolių atvejai Lietuvoje, aptariami Lietuvos teisės aktų, Europos Sąjungos direktyvų ir reglamentų taikymas, bei kitos įgyvendinamos priemonės, skirtos atremti šių hibridinių grėsmių keliamus iššūkius Lietuvos nacionaliniam saugumui.

3.1 Meteorologinių balionų atvejo analizė

Pastaraisiais metais meteorologinių balionų naudojimas gabenant akcizais apmokestintas prekes, o būtent kontrabandines cigaretes iš Baltarusijos į Lietuvą, tapo ne tik teisėsaugos institucijų, tačiau ir Lietuvos nacionalinio saugumo problema. Šis reiškinys parodė, kad netradiciniai ir sunkiai kontroliuojami veikimo būdai gali būti naudojami ne tik ekonominei naudai gauti, tačiau ir kaip hibridinė ataka skirta apkrauti valstybės saugumo sistemą, tikrinti jos pasiruošimą, reagavimo pajėgumus, destabilizuoti visuomenę, bei didinti jos nepasitikėjimą valstybinėmis institucijomis, mažinti gyventojų saugumo jausmą. Ypač reikšminga tai, kad meteorologinių balionų keliama grėsmė, ėmė tiesiogiai veikti strateginės reikšmės objektų funkcionavimą. Dėl į Lietuvos oro erdvę įskridusių meteorologinių balionų, oro uostų darbas pradėjo būti trikdomas. Tai reiškia ne tik laikinuosius veiklos apribojimus, bet ir platesnes pasekmes valstybės saugumo sistemai. Iš pradžių, vertinta kaip įprasta nusikalstama veika, meteorologinių balionų problema peržengė įprastos kontrabandos ribas ir tapo iššūkiu valstybės gebėjimui užtikrinti kritinės infrastruktūros apsaugą, viešąją tvarką, visuomenės saugumą ir veiksmingą reagavimą į iškilusias hibridines grėsmes. Lietuvos Respublikos Vyriausybės

[135] Valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, *Grėsmių nacionaliniam saugumui vertinimas,* (Vilnius, 2026), 6, https://www.vsd.lt/wp-content/uploads/2026/03/2026-GR-LT-El_NAUJAS.pdf.

tinklapyje nurodoma, kad *„Baltarusijos režimas sistemingai pažeidžia Lietuvos oro erdvę [...]. Tai – hibridinė ataka prieš Lietuvą, jos civilinę aviaciją ir visuomenę“.*[136]

Sparčiai didėjančią šio reiškinio tendenciją rodo Valstybės sienos apsaugos tarnybos pateikta statistika, kurioje matyti, kad cigarečių transportavimas, per valstybės sieną oru, išlieka dažniausiai kontrabandininkų naudojamu būdu. 2025 metais, nustatytų atvejų skaičius siekė 652 kartų, tuo tarpu 2024 metais, perpus mažiau – 318 kartų.[137] Palyginimui, 2023 metais tokių atveju skaičius siekė viso labo 3 kartus, o 2022 metais tokių atvejų nebuvo fiksuota iš viso.[138]

Dėl meteorologinių balionų įskrendančių į Lietuvos oro uostų prieigas, 2025 m. spalio 4 – gruodžio 12 d. laikini oro erdvės ribojimai virš Vilniaus oro uosto, buvo įvesti 15 kartų, ir vieną kartą Kauno oro uoste. Oro erdvės ribojimai paveikė daugiau nei 350 skrydžių ir apie 51 tūkst. keleivių. Lietuvos oro uostai kartu su savo partneriais patyrė virš 750 tūkst. eurų nuostolių.[139]

Reaguojant į naujai iškilusią grėsmę ir stengiantis užtikrinti aviacijos, kritinės infrastruktūros tinkamą apsaugą, 2024 metų lapkričio 12 d., buvo atlikti Lietuvos Respublikos aviacijos įstatymo Nr. VIII-2066 2 ir 18 straipsnių pakeitimai.[140] Minėtais pakeitimas buvo įtvirtinta, kad bepiločių orlaivių sistemų geografinės zonos, kuriose visi arba kai kurie bepiločių orlaivių skrydžiai draudžiami, gali būti nustatomos ne tik virš teritorijų, kuriose yra nacionaliniam saugumui užtikrinti svarbios įmonės, kritinės infrastruktūros objektai, valstybės institucijos, tačiau ir miesto gyvenamojoje vietovėje 1 kilometro atstumu arba kaimo gyvenamojoje vietovėje 3 kilometrų atstumu nuo tokių objektų teritorijos. Iki šių pakeitimų, bepiločių orlaivių neskraidymo zonos galėjo būti nustatomos tik virš kritinės infrastruktūros objektų, tačiau ne tam tikru spinduliu aplink juos.[141]

Valstybei toliau sistemingai reaguojant į meteorologinių balionų keliamas grėsmes, Lietuvos Respublikos Vyriausybės 2025 m. lapkričio 12 d. nutarimu Nr. 782 *„atsižvelgiant į neatidėliotinai iškilusį poreikį griežtinti baudžiamąją atsakomybę siekiant užkardyti kontrabandos*

---

[136] „Hibridinė Baltarusijos ataka prieš Lietuvą“, Lietuvos Respublikos Vyriausybė, žiūrėta 2026 m. kovo 23 d., https://lrv.lt/lt/hibridine-baltarusijos-ataka-pries-lietuva.

[137] Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos, 2025 metų veiklos ataskaita, (Vilnius, 2026), 10, https://vsat.lrv.lt/public/canonical/1773657041/6190/2025%20m.%20VSAT%20veiklos%20ataskaita.pdf.

[138] „Antradienį perimtos 7 iš Baltarusijos oro balionais skraidintos rūkalų siuntos (video)“, Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos, žiūrėta 2026 m. kovo 23 d., https://vsat.lrv.lt/lt/naujienos/antradieni-perimtos-7-is-baltarusijos-oro-balionais-skraidintos-rukalu-siuntos-video-bfc.

[139] „Bartkus patikino: daugiau aviakompanijų keisti krypčių dėl balionų neplanuoja“, Lietuvos nacionalinis radijas ir televizija, žiūrėta 2026 m. kovo 23 d., https://www.lrt.lt/naujienos/verslas/4/2773256/bartkus-patikino-daugiau-aviakompaniju-keisti-krypciu-del-balionu neplanuoja?srsltid=AfmBOopxqEGUIm6MGJUfGJbUdqsBohYKqiPxyMWfH-xCsB84r652jSoE.

[140] „Lietuvos Respublikos aviacijos įstatymo Nr. VIII-2066 2 ir 18 straipsnių pakeitimo įstatymas“, TAR, žiūrėta 2026 m. balandžio 15 d., https://www.e-tar.lt/portal/lt/legalAct/dac62e32a8b611ef90b5ee8931e5ce5e.

[141] „Seimas pritarė siūlymams dėl bepiločių orlaivių ir kitų skraidančių objektų kontrolės stiprinimo“, Lietuvos Respublikos Seimas, žiūrėta 2026 m. balandžio 15 d., https://www.lrs.lt/sip/portal.show?p_r=35435&p_t=290018&printVersion=1.

ar kitų krovinių gabenimo atvejus, kai tai vykdoma pažeidžiant teisės aktų nustatytas specialias elgesio saugumo taisykles ir dėl to kyla pavojus nacionaliniam ir visuomenės saugumui [...]“[142], Lietuvos Respublikos Seimui skubos tvarka, buvo perduoti svarstyti įstatymų projektai, susiję su Lietuvos Respublikos baudžiamojo kodekso 199, 199^2, 253^2, 256^2, 260^1, 266^1, 267^2, 267^3, 276^4 ir 282^1 straipsnių pakeitimais. Aiškinamajame rašte, pagrindine įstatymų pakeitimų priežastimi įvardijamas kontrabandos gabenimo masto augimas: per pirmuosius devynis 2025 metų mėnesius daugiau, negu keturi penktadaliai iš Baltarusijos į Lietuvą patekusių cigarečių buvo atgabentos būtent oru, naudojant oro balionus ar kitus bepiločius orlaivius. Meteorologiniai balionai, skrisdami į oro uostų erdvę, trikdo Vilniaus ir Kauno oro uostų darbą, todėl aviacijos sektorius patiria finansinę ir reputacinę žalą, o atšaukiami skrydžiai kelia visuomenės nepasitenkinimą, o tokių atvejų masiškumas, mažina visuomenės saugumo jausmą.[143]

Atsižvelgiant į tai, 2025 m. gruodžio 11 d. įstatymu Nr. XV-655 buvo sugriežtinta baudžiamoji atsakomybė už įvairaus pobūdžio kontrabandą, kuri įtvirtinta Lietuvos Respublikos baudžiamojo kodekso (toliau LR BK) 199, 253^2, 256^2, 260^1, 266^1, 267^2, 267^3, 276^4 straipsniuose, taip pat akcizais apmokestinamų prekių neteisėtą disponavimą, numatytą LR BK 199^2 straipsnyje ir transporto eismo tvarkos ar saugumo taisyklių pažeidimą, numatytą LR BK 282 straipsnyje. Žemiau esančioje lentelėje, pateikiama minėtų baudžiamojo kodekso pakeitimų analizė.

4 lentelė. LR Baudžiamojo kodekso pakeitimai, reaguojant į meteorologinių balionų grėsmes

Baudžiamojo kodekso straipsnis	Atlikti pakeitimai
199 str. Kontrabanda	**Straipsnis buvo papildytas nauja, 4 dalimi:** *„Tas, kas per Lietuvos Respublikos valstybės sieną gabendamas privalomus pateikti muitinei daiktus nepateikė jų muitinės kontrolei ar kitaip šios kontrolės išvengė, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo dvejų iki aštuonerių metų.“* **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
199^2 str. Neteisėtas disponavimas akcizais apmokestinamomis prekėmis	**Straipsnis buvo papildytas nauja, 4 dalimi:** *„Tas, kas pažeisdamas nustatytą tvarką įgijo, laikė, gabeno, siuntė, naudojo ar realizavo akcizais apmokestinamas prekes, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo dvejų iki*

[142] „Nutarimas „Dėl Lietuvos Respublikos baudžiamojo kodekso 199, 199^2, 253^2, 256^2, 260^1, 266^1, 267^2, 267^3, 276^4 ir 282^1 straipsnių pakeitimo įstatymo, Lietuvos Respublikos kriminalinės žvalgybos įstatymo 8 straipsnio pakeitimo įstatymo projektų pateikimo“, TAR, žiūrėta 2026 m. kovo 23 d., https://www.e-tar.lt/portal/lt/legalAct/d26f05b0c0aa11f092fda1fd0c194cc5.

[143] „Aiškinamasis raštas „Dėl Lietuvos Respublikos baudžiamojo kodekso 199, 199^2, 253^2, 256^2, 260^1, 266^1, 267^2, 267^3, 276^4 ir 282 straipsnių pakeitimo įstatymo, Lietuvos Respublikos kriminalinės žvalgybos įstatymo 8 straipsnio pakeitimo įstatymo projektų“, TAR, žiūrėta 2026 m. kovo 23 d., https://www.e-tar.lt/rs/lasupplement/d26f05b0c0aa11f092fda1fd0c194cc5/ff72aa89c0af11f092fda1fd0c194cc5/format/ISO_PDF/?csrt=10097897341412856574.

	aštuonerių metų.“ **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
253[2] str. Šaunamųjų ginklų, šaudmenų, sprogmenų, sprogstamųjų medžiagų ar strateginių prekių kontrabanda	**Straipsnis buvo papildytas nauja, 3 dalimi:** *„Tas, kas padarė šio straipsnio 1 ar 2 dalyje numatytą veiką, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo penkerių iki dešimties metų.“* **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
256[2] str. Branduolinių ar radioaktyviųjų medžiagų arba kitų jonizuojančiosios spinduliuotės šaltinių kontrabanda	**Straipsnis buvo papildytas nauja, 2 dalimi:** „*Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo trejų iki aštuonerių metų.“* **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
260[1] str. Narkotinių ar psichotropinių medžiagų kontrabanda	**Straipsnis buvo papildytas nauja, 5 dalimi:** *„Tas, kas nepateikdamas muitinės kontrolei ar kitaip jos išvengdamas arba neturėdamas leidimo per Lietuvos Respublikos valstybės sieną gabeno ar siuntė narkotines ar psichotropines medžiagas, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo ketverių iki dvylikos metų.“* **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
266[1] str. Pirmos kategorijos narkotinių ar psichotropinių medžiagų pirmtakų (prekursorių) kontrabanda	**Straipsnis buvo papildytas nauja, 3 dalimi:** *„Tas, kas padarė šio straipsnio 1 ar 2 dalyje numatytą veiką, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo ketverių iki septynerių metų.“* **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
267[2] str. Stipriai veikiančių, nuodingųjų ar cheminių medžiagų kontrabanda	**Straipsnis buvo papildytas nauja, 3 dalimi:** „Tas, kas padarė šio straipsnio 1 ar 2 dalyje numatytą veiką, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo trejų iki aštuonerių metų.“ **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
267[3] str. Biologinių medžiagų, mikroorganizmų ar toksinų kontrabanda	**Straipsnis buvo papildytas nauja, 2 dalimi:** „ Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo trejų iki aštuonerių metų.“ **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
276[4] str. Lietuvos Respublikos tam tikrų dopingo medžiagų kontrolės įstatyme nurodytų medžiagų kontrabanda	**Straipsnis buvo papildytas nauja, 2 dalimi:** *„Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką, jeigu tai sukėlė realią grėsmę žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba sutrikdė saugų transporto eismą, arba padarė didelę turtinę žalą, baudžiamas laisvės atėmimu nuo dvejų iki šešerių metų.“* **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**
282 str. Transporto eismo tvarkos ar saugumo taisyklių pažeidimas	**Straipsnis buvo papildytas naujomis dalimis**: *„2. Tas, kas neteisėtai panaudojo valdomą ar nevaldomą objektą, judantį oru, žeme ar vandeniu, ir dėl to kilo reali grėsmė žmogaus gyvybei ar sveikatai, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai*

	arba buvo sutrikdytas saugus transporto eismas, arba padaryta didelė turtinė žala, baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki šešerių metų.”, taip pat *„3. Tas, kas padarė šio straipsnio 2 dalyje numatytą veiką, jeigu dėl to buvo sunkiai sutrikdyta žmogaus sveikata arba buvo padaryta labai didelė turtinė žala, arba atsirado kitokių sunkių padarinių,* *baudžiamas laisvės atėmimu nuo trejų iki dešimties metų.” ir „ 4. Tas, kas padarė šio straipsnio 2 dalyje numatytą veiką, jeigu dėl to žuvo žmogus, baudžiamas laisvės atėmimu nuo aštuonerių iki dvidešimties metų arba laisvės atėmimu iki gyvos galvos.“, bei „6. Už šio straipsnio 2, 3 ir 4 dalyse numatytas veikas atsako ir juridinis asmuo.*“ **Kitose straipsnio dalyse įtvirtinti bausmių dydžiai, pakeisti nebuvo.**

Šaltinis: Sudaryta darbo autoriaus, remiantis *„2000 m. rugsėjo 26 d. Nr. VIII-1968 Lietuvos Respublikos baudžiamuoju kodeksu“*.[144]

Kaip matome, analizuojami baudžiamojo kodekso straipsniai, susiję su kontrabanda ir akcizais apmokestintų prekių gabenimu, buvo papildyti naujomis kvalifikuotomis nusikalstamų veikų sudėtimis, kurių kvalifikuojantys požymiai siejami su realiai kilusia grėsme sutrikdyti žmogaus gyvybę ar sveikatą, nacionaliniam saugumui užtikrinti svarbios įmonės veiklą arba sutrikdyti saugų transporto eismą, ar didele turtine žala. LR BK 282 straipsnyje atsirado trys naujos kvalifikuotos nusikalstamų veikų sudėtys, susijusios su neteisėtu valdomo ar nevaldomo objekto panaudojimu, žeme, vandeniu ar oru, jeigu dėl to kilo reali grėsmė žmonių sveikatai ar gyvybei, nacionaliniam saugumui užtikrinti svarbios įmonės veiklai arba buvo sutrikdytas saugus transporto eismas, arba padaryta didelė turtinė žala, taip pat jeigu buvo sunkiai sutrikdyta žmogaus sveikata, ar padaryta labai didelė turtinė žala arba atsirado kitokių sunkių padarinių, arba dėl to žuvo žmogus.[145] Visų nurodytų straipsnių, išskyrus 282 straipsnį, dispozicijose, numatytos realios laisvės atėmimo bausmės nuo dvejų, iki dešimties metų. LR BK 282 straipsnio dispozicijoje numatytos ir kitos bausmių rūšys: bauda, laisvės apribojimas, areštas, laisvės atėmimas nuo trejų metų iki dešimties metų, arba laisvės atėmimas iki gyvos galvos.

Labai svarbu paminėti ir tai, kad LR BK 199^2 str. 4 dalyje nėra nurodoma akcizais apmokestintų prekių vertė, todėl baudžiamoji atsakomybė, susijusi su realia laisvės atėmimo bausme nuo šiol kyla ir tais atvejais, kai akcizinių prekių kontrabanda yra gabenama nedideliais kiekiais, tačiau pavojingu būdu.[146] Išanalizavus Lietuvos Respublikos administracinių nusižengimų kodekse numatytą atsakomybę už kontrabandą, nustatyta, kad jokių pakeitimų, susijusių su meteorologiniais balionais ar kitomis hibridinėmis grėsmėmis, administracinių

[144] „Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas“, TAR, žiūrėta 2026 m. kovo 24 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr?csrt=7351734137272631161.
[145] Andrius Nevera, „2025 m. Baudžiamojo kodekso pokyčiai ir jų vertinimas“, *Lietuvos teisė 2025: esminiai pokyčiai* (Vilnius: Mykolo Romerio universitetas, 2025), 49, https://cris.mruni.eu/cris/handle/007/50581.
[146] Ibid, 64.

nusižengimų kodekse atlikta nebuvo. Taigi, nuo šiol ir už nedidelį kiekį kontrabandos, kuri gabenama pavojingu būdu, yra taikoma griežčiausia, t.y. baudžiamoji atsakomybė.

Svarbu aptarti ir glaudžiai susijusio, LR BK 118 straipsnio, numatančio atsakomybę už padėjimą kitai valstybei veikti prieš Lietuvos Respubliką, atliktus pakeitimus. Nuo 2003-05-01 galiojusioje straipsnio redakcijos pirmojoje dalyje, iki pakeitimu buvo numatyta, kad *„tas, kas padėjo kitai valstybei ar jos organizacijai veikti prieš Lietuvos Respubliką - jos konstitucinę santvarką, suverenitetą, teritorijos vientisumą, gynybos ar ekonomikos galią, baudžiamas laisvės atėmimu iki septynerių metų.“*[147] 2022 m. gegužės 24 d., įstatymu Nr. XIV-1117, 118 straipsnio pirmosios dalies sankcija buvo sugriežtinta, nustatant minimalų laisvės atėmimo bausmės laikotarpį nuo dvejų metų. Taip pat, straipsnis buvo papildytas ir visiškai naujomis antra, trečia ir ketvirta dalimis. Naująja straipsnio antra dalimi, buvo numatytas asmens atleidimas nuo baudžiamosios atsakomybės, jeigu *„jis iki jo pripažinimo įtariamuoju prisipažino padaręs nusikalstamą veiką ir aktyviai bendradarbiavo nustatant užsienio valstybės ar jos organizacijos atstovus ir jų vykdomą veiklą, nukreiptą prieš Lietuvos Respublikos konstitucinę santvarką, suverenitetą, teritorijos vientisumą, gynybos ar ekonomikos galią.“*[148] Naujoje trečioje dalyje, numatyta, kad *„šio straipsnio 2 dalis netaikoma asmeniui, kuris šiame straipsnyje ar šio kodekso 119 straipsnyje nustatytais pagrindais nuo baudžiamosios atsakomybės jau buvo atleistas, taip pat jeigu dėl šio straipsnio 1 dalyje numatytos veikos padarymo žuvo žmogus ar atsirado kitokių sunkių padarinių.“*[149], o straipsnio ketvirta dalimi numatyta atsakomybė jau ir juridiniam asmeniui. 2024 m. birželio 6 d. įstatymu Nr. XIV-2683, 118 straipsnis, buvo papildytas nauja kvalifikuojančia, nusikalstamos veikos pavojingumą didinančia sudėtimi, numatant griežtesnę baudžiamąją atsakomybę už padėjimą veikti prieš Lietuvos Respubliką, pasinaudojant ekstremaliąja situacija, nepaprastąja padėtimi ar mobilizacija. Už tokią nusikalstamą veiką, numatytas laisvės atėmimas nuo trejų iki dešimties metų.[150]

Taigi, galima teigti, jog atlikti baudžiamojo kodekso pakeitimai yra tiesiogiai susiję su naujai atsiradusiu, meteorologinių balionų reiškiniu, kurie kelia grėsmę šalies nacionaliniam saugumui ir yra laikoma hibridine Baltarusijos ataka prieš Lietuvą. Pavojingu būdu vykdomos kontrabandos atvejai, buvo atriboti nuo įprastos, administracinės atsakomybės ribose vykusios kontrabandos ir perkelti į baudžiamosios teisės reguliavimo sritį. Taip pat, LR BK 118 straipsnis buvo papildytas naujomis dalimis, straipsnio 1 dalies sankcija buvo sugriežtinta, įtraukta nauja

[147] „2000 m. rugsėjo 26 d. Nr. VIII-1968 Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas“, TAR, žiūrėta 2026 m. balandžio 20 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/wZXqTUOQzz.
[148] „Lietuvos Respublikos baudžiamojo kodekso 9-1, 118 ir 119 straipsnių pakeitimo įstatymas“, TAR, žiūrėta 2026 m. balandžio 20 d., https://e-tar.lt/portal/lt/legalAct/7bfd8700e1ac11ec8d9390588bf2de65.
[149] *Ibid*.
[150] „Lietuvos Respublikos baudžiamojo kodekso 114, 118, 119, 120 ir 121 straipsnių pakeitimo įstatymas”, TAR, žiūrėta 2026 m. balandžio 20 d., https://www.e-tar.lt/portal/lt/legalAct/8e1931e0299011efbdaea558de59136c.

kvalifikuojanti, veikos pavojingumą didinanti, sudėtis. Vis dėl to, vienareikšmiškai teigti, jog baudžiamojo kodekso pakeitimai turi įtakos šios hibridinės atakos masiškumui, kol kas negalima, dėl neilgo, naujai įsigaliojusio baudžiamojo kodekso veikimo laikotarpio.

Toliau analizuojant Lietuvos teisinio reglamentavimo pasikeitimus, matyti, jog buvo išplėsti ir Policijos įstatyme numatyti pareigūnų įgaliojimai, susiję su prievartos, šaunamųjų ginklų bei sprogmenų panaudojimu. Policijos įstatymo 27 straipsnio, numatančio prievartos naudojimo sąlygas, 1 dalis, 3 dalies 6 punktas ir 28 straipsnio, numatančio šaunamųjų ginklų ir sprogmenų naudojimą, 1 ir 3 dalys, 2024 m. lapkričio 12 d. įstatymu Nr. XIV-3136, buvo papildytos. Po atliktų pakeitimų, policijos pareigūnai, remiantis 27 str. 1 d., nuo šiol turi teisę panaudoti prievartą ir tada, kai *„[...] bet koks delsimas kelia pavojų pareigūno ar kito asmens gyvybei, sveikatai ar turtui arba aviacijos saugumui, Lietuvos Respublikos valstybės sienos apsaugai, nacionaliniam saugumui užtikrinti svarbioms įmonėms, nacionaliniam saugumui užtikrinti svarbiems įrenginiams ir turtui ar kitiems pareigūno saugomiems objektams.“*[151]. Iki šio pakeitimo, minėto straipsnio 1 dalyje, nebuvo minimas aviacijos saugumas, valstybės sienos apsauga ar nacionaliniam saugumui užtikrinti svarbių įmonių apsauga. Taip pat, pakeitimai buvo atlikti ir to paties straipsnio 3 dalies 6 punkte, kuriuo labiau detalizuoti judančio objekto požymiai, prieš kurį galima panaudoti prievartą: *„autonomiškai arba nuotoliniu būdu valdomą objektą, judantį oru, žemės, vandens paviršiumi arba po vandeniu, (tarnybinio būtinumo atvejais)“.* Iki minėto pakeitimo, pagal 27 str. 3 d. 6 punktą, pareigūnas turėjo teisę panaudoti prievartą stabdydamas transporto priemonę, laivą ar orlaivį.[152] 27 straipsnio 3 dalis, buvo papildyta ir visiškai nauju, 8 punktu, kuriuo remiantis, prievarta gali būti panaudota ir tada, *„kai būtina pašalinti orlaivio, autonomiškai arba nuotoliniu būdu valdomo objekto, judančio oru, žemės, vandens paviršiumi arba po vandeniu, keliamą pavojų aviacijos saugumui, Lietuvos Respublikos valstybės sienos apsaugai, nacionaliniam saugumui užtikrinti svarbioms įmonėms, nacionaliniam saugumui užtikrinti svarbiems įrenginiams ir turtui ar kitiems jo saugomiems objektams.“*[153] 28 straipsnio 1 dalis, reglamentuojanti šaunamųjų ginklų ir sprogmenų naudojimą, taip pat buvo papildyta jau ankščiau minėtais identiškais požymiais. Nuo šiol, pareigūnai gali panaudoti šaunamąjį ginklą ar sprogmenis, kai tai kelia grėsmę *„[...] aviacijos saugumui, Lietuvos Respublikos valstybės sienos apsaugai, nacionaliniam saugumui užtikrinti svarbioms įmonėms, nacionaliniam saugumui užtikrinti svarbiems įrenginiams ir turtui, kitiems pareigūno saugomiems*

[151] „Lietuvos Respublikos policijos įstatymo Nr. VIII-2048 2, 27 ir 28 straipsnių pakeitimo įstatymas“, TAR, žiūrėta 2026 m. kovo 25 d., https://www.e-tar.lt/portal/lt/legalAct/59aaf352a8b411ef90b5ee8931e5ce5e?csrt=1320035902353116754.
[152] „Lietuvos Respublikos policijos įstatymas“, TAR, žiūrėta 2026 m. kovo 25 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.CA89372D00AA/GQPVYLUSox?csrt=1320035902353116754.
[153] „Lietuvos Respublikos policijos įstatymo Nr. VIII-2048 2, 27 ir 28 straipsnių pakeitimo įstatymas“, op.cit.

objektams arba nusikalstamų veikų užkardymui.“[154] To paties straipsnio 3 dalis, buvo pakeista ir papildyta dviem naujais punktais: *„Pareigūnas, nekeldamas tiesioginio pavojaus asmens gyvybei, turi teisę panaudoti šaunamąjį ginklą prieš gyvūną, laivą arba transporto priemonę, kai kyla neišvengiamas pavojus pareigūno arba kitų asmenų gyvybei ar sveikatai. Pareigūnas, nekeldamas tiesioginio pavojaus asmens gyvybei, taip pat turi teisę panaudoti šaunamąjį ginklą prieš orlaivį, autonomiškai arba nuotoliniu būdu valdomą objektą, judantį oru, žemės, vandens paviršiumi arba po vandeniu, šiais atvejais: 1) kai kyla neišvengiamas pavojus pareigūno ar kitų asmenų gyvybei ar sveikatai; 2) užkirsdamas kelią nusikalstamoms veikoms, taip pat kai būtina pašalinti orlaivio, autonomiškai arba nuotoliniu būdu valdomo objekto, judančio oru, žemės, vandens paviršiumi arba po vandeniu, keliamą pavojų aviacijos saugumui, Lietuvos Respublikos valstybės sienos apsaugai, nacionaliniam saugumui užtikrinti svarbioms įmonėms, nacionaliniam saugumui užtikrinti svarbiems įrenginiams ir turtui ar kitiems jo saugomiems objektams.“*[155] Kaip matome, iki atliktų pakeitimų, policijos pareigūnų įgaliojimai buvo orientuoti į tradiciniu būdu judančių objektų kontrolę. Pažymėtina, kad analogiški pakeitimai buvo atlikti ir kitų teisėsaugos institucijų, tokių kaip Valstybės sienos apsaugos tarnybos, Finansinių nusikaltimų tyrimų tarnybos ir kt., turinčių teisę naudoti šaunamuosius ginklus, įstatymuose, siekiant suvienodinti jų veikimą. Po pakeitimų, pareigūnų įgaliojimai buvo labiau detalizuoti ir išplėsti, įtraukiant autonomiškai arba nuotoliniu būdu valdomų objektų keliamos grėsmės neutralizavimą.[156] Tokie pakeitimai vertintini kaip sistemiška valstybės reakcija į didėjantį hibridinių grėsmių pavojų, siekiant užtikrinti veiksmingesnę oro saugumo, valstybės sienos apsaugos bei kritinės infrastruktūros apsaugą.

2025 m. gruodžio 9 d. Lietuvos Respublikos Vyriausybė, remiantis Nacionalinio krizių valdymo centro pateiktu pasiūlymu, priėmė nutarimą *„Dėl valstybės lygio ekstremaliosios situacijos paskelbimo ir valstybės lygio ekstremaliosios situacijos valstybės operacijų vadovo paskyrimo“.*[157] Nutarime nurodyta, kad valstybės lygio ekstremalioji situacija šalyje yra skelbiama „*dėl iš Baltarusijos Respublikos teritorijos į Lietuvos Respublikos teritoriją nuolat leidžiamų ir kontrabandą gabenančių balionų, keliančių grėsmę Lietuvos Respublikos nacionalinio saugumo interesams, bei dėl to kylančio pavojaus žmonių gyvybei, sveikatai, turtui ir (ar) aplinkai.*“[158]

Su aukščiau minėtu nutarimu glaudžiai susijęs ir 2025 m. gruodžio 18 d. Lietuvos Respublikos Seimo priimtas nutarimas *„Dėl teisių kariams suteikimo ekstremaliosios situacijos*

---

[154] *Ibid*.
[155] *Ibid*.
[156] „Vyriausybė pritarė bepiločių orlaivių ir kitų skraidančių objektų kontrolės stiprinimui“, Lietuvos Respublikos Vyriausybė, žiūrėta 2026 m. kovo 25 d., https://vrm.lrv.lt/lt/naujienos/vyriausybe-pritare-bepilociu-orlaiviu-ir-kitu-skraidanciu-objektu-kontroles-stiprinimui/.
[157] „Nutarimas „Dėl valstybės lygio ekstremaliosios situacijos paskelbimo ir valstybės lygio ekstremaliosios situacijos valstybės operacijų vadovo paskyrimo“, TAR, žiūrėta 2026 m. kovo 3 d., https://www.e-tar.lt/portal/lt/legalAct/603808e2d4cb11f08918e1adc7c5b1ec.
[158] *Ibid.*

atveju“[159]*,* kuriuo buvo išplėsti karių įgaliojimai ekstremaliosios situacijos metu, kilusios dėl kontrabandą gabenančių balionų. Įstatymu buvo numatyta, kad kariai „*[...]padeda policijos, Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos ir Viešojo saugumo tarnybos prie Vidaus reikalų ministerijos pajėgoms vykdyti jų funkcijas likviduojant šią ekstremaliąją situaciją ir šalinant jos padarinius, ekstremaliosios situacijos galiojimo laikotarpiui, tačiau ne ilgesniam negu 3 mėnesių terminui [...]*“.[160] Kariai nutarimu įgijo teisę duoti privalomus nurodymus fiziniams ar juridiniams asmenims, persekioti ir sulaikyti asmenis, nevykdančius karių nurodymų arba įtariamus padarius nusikalstamą veiką ar kitą teisės pažeidimą, laikinai apriboti patekimą į tam tikrą teritoriją, uždrausti tr. priemoniu eismą, tikrinti asmenų, tr. priemonių, ginklų ar kitus dokumentus, atlikti asmenų apžiūras ir daiktų patikras, stabdyti, tikrinti ir apžiūrėti tr. Priemones, krovinius, jose esančius daiktus, asmenis ir jų turimą bagažą bei panaudoti specialiąsias priemones.[161]

2025 m. gruodžio 11 d. pakeitimai buvo atlikti ir Lietuvos Respublikos Kriminalinės žvalgybos įstatyme. Šio įstatymo 8 straipsnio 1 dalies 1 punktas buvo papildytas aukščiau minėta, atnaujinta, Lietuvos Respublikos baudžiamojo kodekso 282 straipsnio 2 dalyje numatyta nusikalstama veika, taip suteikiant teisinį pagrindą pradėti kriminalinės žvalgybos tyrimą, kai turima informacijos apie rengiamą, daromą ar padarytą šioje baudžiamojo įstatymo normoje numatytą nusikalstamą veiką transporto saugumo sutrikdymui.[162] Iki šio pakeitimo, kriminalinės žvalgybos veiksmai, dėl LR BK 282 straipsnio 2 dalies, negalėjo būti taikomi.

2025 m. gruodžio 2 d. Vidaus reikalų ministras Vladislavas Kondratovičius, kreipėsi į Europos Komisijos vidaus reikalų ir migracijos komisarą, prašydamas imtis neatidėliotinų veiksmų ir paremti naują sankcijų paketą Baltarusijos pareigūnams ir institucijoms dėl vykdomų intensyvių hibridinių atakų iš Baltarusijos, kuriomis sistemingai pažeidžiama Lietuvos oro erdvė.[163] Atsižvelgiant į Lietuvos institucijų prašymą, 2025 m. gruodžio 15 d., Europos Taryba išplėtė sankcijų taikymo sritį Baltarusijai, apimant hibridines veiklas vykdomas prieš ES valstybes nares. Į sankcijų sąrašą nuo šiol bus įtraukiami ir asmenys, subjektai ar organizacijos, gaunantys naudos iš Baltarusijos vykdomų hibridinių atakų, arba padeda jas vykdyti, organizuoti, kai tokie

[159] „Nutarimas „Dėl teisių kariams suteikimo ekstremaliosios situacijos atveju“, TAR, žiūrėta 2026 m. kovo 3 d., https://www.e-tar.lt/portal/lt/legalAct/404b5fa2dc1911f08918e1adc7c5b1ec.
[160] *Ibid.*
[161] *Ibid*.
[162] „Lietuvos Respublikos kriminalinės žvalgybos įstatymo Nr. XI-2234 8 straipsnio pakeitimo įstatymas“, TAR, žiūrėta 2026 m. kovo 25 d., https://www.e-tar.lt/portal/lt/legalAct/bb385fe0d9b411f08918e1adc7c5b1ec?csrt=17509282981660083539.
[163] „Dėl suintensyvėjusios Baltarusijos hibridinės atakos Lietuva ragina ES imtis ryžtingų priemonių“, Lietuvos Respublikos vidaus reikalų ministerija, žiūrėta 2026 m. kovo 2 d., https://vrm.lrv.lt/lt/naujienos/del-suintensyvejusios-baltarusijos-hibridines-atakos-lietuva-ragina-es-imtis-ryztingu-priemoniu-M9rX/.

veiksmai kenkia ir kelia grėsmę demokratijai, stabilumui ir saugumui Europos Sąjungai, bei jos valstybėms narėms.[164]

Tą, jog meteorologiniai balionai kelią grėsmę Lietuvos nacionaliniam saugumui, patvirtina ir 2025 metų gruodžio 16 d. Lietuvos Kriminalinės policijos biuro surengta plataus masto operacija, kurios metu buvo sulaikyti asmenys, įtariami nusikalstamu susivienijimu vykdyta kontrabanda balionais. Atlikto ikiteisminio tyrimo tikslas *„pažaboti organizuotas nusikalstamas grupes ciniškai organizuojančias ir vykdančias cigarečių kontrabandą gabenamą meteorologiniais balionais, kurios vykdymo būdas kelia pavojų ir rizikas civilinei aviacijai, o taip pat Lietuvos nacionaliniam saugumui ir ekonominiams interesams.“*[165] Vienas iš svarbiausių šio tyrimo aspektų yra tai, jog asmenims buvo pareikšti įtarimai ne tik dėl kontrabandos, neteisėto disponavimo akcizais apmokestinamomis prekėmis, tačiau ir padėjimo kitai valstybei veikti prieš Lietuvos Respubliką, pagal LR BK 118 straipsnį. Tai parodo, jog meteorologiniai balionai nėra įprasta, nusikalstama veika, o yra vertinama kaip hibridinė grėsmė valstybės nacionaliniam saugumui. Taigi valstybė, kovodama su šios naujai iškilusios hibridinės grėsmes iššūkiais, pradeda formuoti naują teismų praktiką, hibridinių grėsmių kontekste.

Tęsiant kovą su meteorologiniais balionais gabenama kontrabanda, nuo 2025 m. lapkričio 24 dienos, buvo pradėti bendri policijos, Valstybės sienos apsaugos, Muitinės kriminalinės tarnybos ir Karo policijos reidai pasienio rajonuose, besiribojančiuose su Baltarusijos pasieniu. Reidams skiriamos papildomos pareigūnų pajėgos, kurių tikslas prevenciškai stabdyti ir tikrinti automobilius, jais vykstančius asmenis ir turimus daiktus. Nuo reidų pradžios, iki 2026 m. kovo 26 dienos, priemonių metu, iš viso buvo patikrinti beveik 50 tūkst. automobilių, 65 tūkst. asmenų, perimta 119 oro balionų, rasta 304 tūkst. kontrabandinių cigarečių pakelių, pradėta 17 ikiteisminių tyrimų.[166]

Sudėtinga ir kompleksinė hibridinių grėsmių prigimtis, verčia valstybę ieškoti naujų priemonių ir pagalbos, į kovą įtraukiant visuomenę bei verslus. Tam 2025 metų spalio mėnesį, Ekonomikos ir inovacijų ministerija paskelbė technologijų ir inovacijų programą, pagal kurią yra pasiruošusi skirti 1 mln. eurų įmonėms, kurios parengs ir pateiks pasiūlymus, kaip išspręsti meteorologinių balionų problemą Lietuvoje. Dalyvauti programoje, buvo kviečiamos įmonės, kurios siūlytų žvalgybos, antidroninines sistemas, kitas informacinių technologijų ar inžinerines

[164] Council of the European Union, „Belarus: Council broadens scope of sanctions regime to cover hybrid activities against EU member states“, žiūrėta 2026 m. kovo 2 d., https://www.consilium.europa.eu/en/press/press-releases/2025/12/15/belarus-council-broadens-scope-of-sanctions-regime-to-cover-hybrid-activities-against-eu-member-states/.

[165] „Policijos ir prokuratūros smūgis „balionų“ konkrabandos organizatoriams“, Lietuvos Kriminalinės policijos biuras, žiūrėta 2026 m. kovo 25 d., https://lkpb.policija.lrv.lt/lt/naujienos/policijos-ir-prokuraturos-smugis-balionu-konkrabandos-organizatoriams-wJa/.

[166] „Prevencinių reidų pasienio rajonuose rezultatai“, Lietuvos Policija, žiūrėta 2026 m. kovo 25 d., https://policija.lrv.lt/lt/naujienos/reidu-pasienyje-rezultatai-kJ96/.

priemones skirtas oro saugumui Lietuvoje.[167] Programa sulaukė nemažo įmonių susidomėjimo, todėl 2026 metų vasario mėnesį, Silvestro Žukausko poligone, vyko pirmieji paruoštų sistemų, skirtų oro erdvės stebėsenai, grėsmių aptikimui ir reagavimo galimybių stiprinimo, bandymai. Vis dėl to, skirtingų įmonių parengtoms priemonėms dar reikalingi patobulinimai, todėl masinė minėtų priemonių gamyba kol kas neprasidėjo.[168]

Iniciatyvos, prisidedant prie šalies nacionalinio saugumo, imasi ir pačios Lietuvoje veikiančios įmonės. 2026 metų kovo mėnesį, Lietuvoje investuojanti įmonė *„Philip Morris Baltic“*, Vyriausybei perdavė 7 industrinius dronus, skirtus pasienio kontrolei ir kovai su kontrabanda. Premjerės I. Ruginienės teigimu, perduoti dronai žymiai prisidės prie valstybės sienos apsaugos nuo neteisėtai ją kertančių meteorologinių balionų.[169]

Atsaką į iškilusias hibridinės grėsmės, bando pateikti ir pati visuomenė. Lietuvis programuotojas, bendradarbiaudamas kartu su meteorologu, sukūrė programėlę – kalendorių *„NoBalloons“*, kuri pagal vėjo kryptį, bando nuspėti tikimybę, ar vėjas bus palankus skristi meteorologiniams balionams iš Baltarusijos. Pagal tai, galima vertinti, ar bus sutrikdyta Vilniaus oro uosto veikla ir planuoti savo keliones.[170]

Darytina išvada, kad meteorologinių balionų naudojimas gabenant akcizais apmokestinamas prekes iš Baltarusijos į Lietuvą peržengė tradicinės kontrabandos ribas, įgijo hibridinių grėsmių pobūdį ir tapo tikru iššūkiu Lietuvos nacionaliniam saugumui. Lietuvos valstybės atsakas į šią grėsmę yra kompleksinis, apimantis tiek teisės aktų pakeitimus, tiek ir krizių valdymo, tarpinstitucinio bendradarbiavimo, bei kitų priemonių įgyvendinimo visumą: LR Baudžiamojo kodekso straipsniai, susije su kontrabanda, buvo papildyti naujomis kvalifikuotomis nusikalstamų veikų sudėtimis, LR Baudžiamojo kodekso 118 straipsnis buvo papildytas naujomis dalimis, susijusiomis su padėjimu veikti prieš valstybę, to paties straipsnio 1 dalies sankcija buvo sugriežtinta, įtraukta nauja kvalifikuojanti, veikos pavojingumą didinanti, sudėtis, LR Kriminalinės žvalgybos įstatymo 8 straipsnio 1 dalies 1 punktas papildytas LR Baudžiamojo kodekso 282 straipsnio 2 dalyje numatyta nusikalstama veika, valstybėje paskelbta ekstremalioji

[167] „EIMIN skelbia iki 1 mln. eurų vertės programą – siekia greitų technologinių sprendimų oro erdvės saugumui“, Lietuvos Respublikos ekonomikos ir inovacijų ministerija, žiūrėta 2026 m. balandžio 8 d., https://eimin.lrv.lt/lt/ziniasklaidai/naujienos/eimin-skelbia-iki-1-mln-euru-vertes-programa-siekia-greitu-technologiniu-sprendimu-oro-erdves-saugumui-Q0XR/.

[168] „Išbandomi gaminiai, padėsiantys kovoti su kontrabandiniais balionais: ko galime tikėtis“, Lietuvos nacionalinis radijas ir televizija, žiūrėta 2026 m. balandžio 8 d., https://www.lrt.lt/naujienos/lietuvoje/2/2843380/isbandomi-gaminiai-padesiantys-kovoti-su-kontrabandiniais-balionais-ko-galime-tiketis?srsltid=AfmBOoqxP8LmMAyjuJVLR-maKWwclj0ioSSXTr5KaY4di91PxYJFvc_S.

[169] „Vyriausybei JAV investuotojas perdavė technologiją kovai su kontrabandiniais balionais“, Lietuvos Respublikos Vyriausybė, žiūrėta 2026 m. balandžio 8 d., https://lrv.lt/lt/naujienos/vyriausybei-jav-investuotojas-perdave-technologija-kovai-su-kontrabandiniais-balionais-ale8/.

[170] „Sukurtas įrankis, skaičiuojantis tikimybę, kad oro uostą pasieks kontrabandiniai balionai“, Lietuvos nacionalinis radijas ir televizija, žiūrėta 2026 m. balandžio 8 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/2762172/sukurtas-irankis-skaiciuojantis-tikimybe-kad-oro-uosta-pasieks-kontrabandiniai-balionai?srsltid=AfmBOooU5pOhK_hwcstGoAgHo1nCElRdJJNVj_STyQdqAqBEexd8itZr.

situacija, praplėsti karių įgaliojimai, išplėstos statutinių pareigūnų teisės panaudoti šaunamąjį ginklą ar sprogmenis prieš autonomiškai arba nuotoliniu būdu valdomą objektą, pradėti bendri policijos, VSAT, Karo policijos ir kitų institucijų reidai pasienio ruožuose. Atlikti pakeitimai rodo, jog teisinis reguliavimas turi prisitaikyti prie kylančių grėsmių, ir šiai dienai nėra pakankamas. Atsakas į hibridines grėsmes reikalauja priemonių visumos, todėl reaguojant į šią iškilusią grėsmę ir ieškant sprendimo būdų, į procesą yra įtrauktas verslas ir pati visuomenė.

3.2 Kibernetinių išpuolių analizė

Sparčiai vykstanti skaitmenizacija, kurios metu į elektroninę erdvę yra perkeliama vis daugiau kasdien naudojamų ir reikalingų paslaugų, bei augant kritinės infrastruktūros priklausomybei nuo skaitmeninių tinklų, lemia ne tik naujas veiklos galimybes, tačiau ir didesnį pažeidžiamumą kibernetinėje erdvėje. Valstybės saugumo departamentas nurodo, kad *„priešiškų valstybių žvalgybos tarnybos prieš Lietuvą vykdo kibernetinės žvalgybos operacijas, kuriomis siekia perimti žvalgybai vertingą informaciją, destabilizuoti padėtį šalyje ir paveikti visuomenę.“*[171] Atsižvelgiant į tai, kibernetinis saugumas Lietuvoje pastaraisiais metais tapo viena svarbiausių nacionalinio saugumo politikos sričių. Krašto apsaugos viceministro T. Godliausko teigimu *„Kibernetinių incidentų augimas atskleidžia, kad kibernetinis saugumas yra neatsiejama nacionalinio saugumo dalis. Didėjanti geopolitinė įtampa, hibridinės atakos, šnipinėjimas ir povandeninės infrastruktūros pažeidimai Baltijos jūroje rodo, kad stabilumas ir taika nėra savaime suprantami“*[172]. Įvairūs kibernetiniai išpuoliai tampa ypač veiksminga netiesioginio poveikio priemone, leidžianti priešiškai nusiteikusiems subjektams daryti žalą valstybei, neperžengiant ginkluoto konflikto ribų.[173] *„Priešiškos valstybės, nusikaltėliai, kiti piktavaliai vis dažniau naudoja ne tik įprastus ginklus, bet ir naujausias technologijas, pavyzdžiui, dirbtinį intelektą, socialinę inžineriją, dezinformaciją ir propagandą. Šie įrankiai skirti kritinei infrastruktūrai pažeisti, svarbioms paslaugoms sutrikdyti, pasitikėjimui institucijomis mažinti, visuomenei skaldyti ir nesaugumo jausmui kurti“*[174]. Pavyzdžiui, 2022 m. birželio 29 d. buvo sutrikdytos daugiau kaip 137 Lietuvos valstybės institucijų ir verslo interneto svetainės. Atsakomybę už šias atakas prisiėmė su Rusijos žvalgyba siejama grupuotė „Killnet“.[175] Kiti

[171] „Kaip vykdoma kibernetinė žvalgyba?“, Lietuvos Respublikos Valstybės saugumo departamentas, žiūrėta 2026 m. balandžio 6 d., https://www.vsd.lt/verbavimas/kaip-vykdoma-kibernetine-zvalgyba.
[172] „Nacionalinė kibernetinio saugumo būklės ataskaita: pernai 63 proc. išaugo kibernetinių incidentų skaičius”, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 4 d., https://www.nksc.lt/naujienos/nacionaline_kibernetinio_saugumo_bukles_ataskaita_.html.
[173] Lietuvos Respublikos krašto apsaugos ministerija, *Lietuvos kibernetinio saugumo būklės apžvalga: svarbiausia informacija 2024*, žiūrėta 2026 m. balandžio 4 d., https://kam.lt/wp-content/uploads/2025/07/Nacionalines-kibernetinio-saugumo-bukles-ataskaitos-santrauka-2024.pdf.
[174] *Ibid*.
[175] Lietuvos Respublikos krašto apsaugos ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita 2022* (Vilnius, 2022), 61, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf.

kibernetinio išpuolio, kaip hibridinės atakos pavyzdžiai, buvo užfiksuoti 2023 metais, kurių metu buvo sutrikdyta muzikos transliacija radijo stotyje ir prekybos centre, kuomet pakeitus grojaraštį buvo pradėta transliuoti dezinformacija. Tokio tipo hibridinės atakos Lietuvoje fiksuotos ne pirmą kartą.[176] Kibernetinių atakų skaičius Europoje 2023–2024 metais išaugo, bei tapo vis sudėtingesnės. Taikiniu dažniausiai pasirenkamas smulkusis ir vidutinis verslas ar viešasis sektorius, o dėl įtemptos geopolitinės situacijos taikiniu tampa ir kritinė infrastruktūra.[177] Priešiška informacinė veikla prieš Lietuvą vykdoma jau ne vienerius metus, tačiau žymus jos suintensyvėjimas pastebėtas 2024 metais dėl besitęsiančios Rusijos agresijos Ukrainoje.[178] 2024 metais Nacionalinis kibernetinio saugumo centras (toliau NKSC) iš viso užregistravo 3874 kibernetinius incidentus. Palyginimui, 2023 metais, tokių registruotų incidentų skaičius siekė 2378, t. y. apie 63% mažiau. Didžioji dalis jų buvo priskirti nereikšmingai ir vidutinei kategorijoms, tačiau 3 kibernetiniai incidentai buvo priskirti didelei kategorijai ir buvo siejami su užsienio šalių remiamomis grupuotėmis, kurios įsilaužusios į organizacijų tinklus siekia ilgalaikių tikslų, tokių kaip šnipinėjimas.[179]

Verta paminėti ir 2023 metų spalio mėnesį įvykusią koordinuotą ataką, kurios metu švietimo įstaigos visoje Lietuvoje per dieną sulaukė apie 850 pranešimų rusų kalba apie užminuotus darželius ir mokyklas. Analogiški pranešimai buvo išplatinti ir Latvijoje bei Estijoje.[180] *„Melagingais pranešimais ir panašaus pobūdžio veiksmais siekiama kelti įtampą ir paniką visuomenėje, trikdyti ir destabilizuoti institucijų darbą, didinti nepasitikėjimą. Išaugus geopolitinei įtampai, Lietuva ir kitos Baltijos šalys yra nuolatiniai priešiškų valstybių informacinių-kibernetinių atakų taikiniai. [...]“*[181]. Toks pranešimų kiekis per ypač trumpą laiką, pareikalavo didžiulių valstybinių institucijų pajėgumų, ypač policijos, tikrinant gautus pranešimus, evakuojant mokymo įstaigas.

Kibernetinių išpuolių, nutaikytų į kritinę infrastruktūrą, padidėjimas pastebimas visame Baltijos jūros regione. NKSC bendradarbiaudami su užsienio partneriais atliko grėsmių analizę ir nustatė, jog priešiškai nusiteikusių valstybių veiksmai intensyvėja, todėl būtinas didesnis regiono

[176] „NKSC fiksavo du kibernetinius incidentus, susijusius su muzikos transliacijomis“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 4 d., https://www.nksc.lt/naujienos/nksc_fiksavo_du_kibernetinius_incidentus_susijusiu.html.
[177] Lietuvos Respublikos krašto apsaugos ministerija, „Atnaujintas kibernetinio saugumo įstatymas“, žiūrėta 2026 m. balandžio 4 d., https://kam.lt/wp-content/uploads/2024/10/Atnaujintas-kibernetinio-saugumo-istatymas.pdf.
[178] Lietuvos Respublikos krašto apsaugos ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita 2024* (Vilnius, 2025), 82, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2024.pdf.
[179] *Ibid*., 8.
[180] „Policijai gavus 850 grasinimų susprogdinti įstaigas, Požėla ragina nepanikuoti: tai yra koordinuota ataka“, Lietuvos nacionalinis radijas ir televizija, žiūrėta 2026 m. balandžio 14 d., https://www.lrt.lt/naujienos/lietuvoje/2/2099522/policijai-gavus-850-grasinimu-susprogdinti-istaigas-pozela-ragina-nepanikuoti-tai-yra-koordinuota-ataka.
[181] „NKVC atidžiai stebi situaciją dėl platinamų grasinančių pranešimų ugdymo įstaigoms ir teikia rekomendacijas“, Lietuvos Respublikos Vyriausybė, žiūrėta 2026 m. balandžio 14 d., https://lrv.lt/lt/naujienos/nkvc-atidziai-stebi-situacija-del-platinamu-grasinanciu-pranesimu-ugdymo-istaigoms-ir-teikia-rekomendacijas/.

šalių įsitraukimas ir bendradarbiavimas stiprinant kibernetinę gynybą. Dažniausiai, 2024 metais buvo vykdomos paskirstytų paslaugų trikdymo atakos (angl. DDos), bei svetainių turinio pakeitimas (angl. website defacement).[182] Regiono saugumui grėsmę kelia valstybių, dažniausiai Rusijos, remiamos grupuotės, haktivistai ir nusikalstamos grupuotės. Tokių išpuolių motyvai yra skirtingi, pradedant nuo šnipinėjimo, sabotažo ir visuomenės destabilizacijos, baigiant finansinės naudos ar politinės įtakos siekiu. Dažniausiai atakomis yra taikomasi į gyvybiškai svarbius regiono stabilumo ar ekonominius sektorius – naftos, dujų, transporto ar komunikacinius tinklus.[183]

Reaguojant į ženkliai padidėjusį grėsmių skaičių, Krašto apsaugos ministerija formuoja kryptingą kibernetinio saugumo politiką, kuria siekiama užtikrinti Lietuvos atsparumą ir pasirengimą bet kokioms grėsmėms kibernetinėje erdvėje.[184] Atsižvelgiant į tai, 2024 metais spalio 18 d., Lietuvoje įsigaliojo atnaujintas Kibernetinio saugumo įstatymas, kuris *„[...] nustato kibernetinio saugumo principus, kibernetinio saugumo politiką formuojančias ir ją įgyvendinančias institucijas, jų funkcijas ir įgaliojimus, kibernetinio saugumo subjektų identifikavimo pagrindus ir šių subjektų pareigas, keitimąsi informacija ir tarpinstitucinį bendradarbiavimą, kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams patikrinimus ir vykdymo užtikrinimo priemones, nacionalinės kibernetinio saugumo sertifikavimo institucijos įgaliojimus, Saugiojo valstybinio duomenų perdavimo tinklo naudojimo pagrindus“.*[185] Įstatymo **4 straipsnis** nurodo, kad Lietuvos policija, Nacionalinis kibernetinio saugumo centras ir Valstybinė duomenų apsaugos inspekcija yra pagrindinės valstybinės institucijos, atsakingos už kibernetinio saugumo politikos įgyvendinimą Lietuvoje.[186] Vienas iš svarbiausių atnaujinto įstatymu pasikeitimų - į Lietuvos nacionalinę teisę perkelta nauja **Europos Sąjungos Tinklų ir informacinių sistemų direktyva (TIS 2)**. Direktyva nustato bendrą teisinę sistemą tarp valstybių narių, kuria siekiama užtikrinti kibernetinį saugumą 18-oje ypatingos svarbos sektorių visoje ES, pavyzdžiui energetikos, transporto, sveikatos priežiūros, finansų ir k.t. Direktyvoje numatyta, būtinybė stiprinti kibernetinio saugumo pajėgumus, apibrėžti nacionalines kibernetinio saugumo strategijas ir bendradarbiauti tarpusavyje su kitomis ES šalimis tarpvalstybinio reagavimo srityje.[187] Direktyvos 6 punktu taip pat numatyta, kad jos taikymo sritis turėtų būti praplėsta,

[182] „Baltijos jūros regiono šalyse dažnėja kibernetinės atakos nutaikytos į kritinę infrastruktūrą“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 4 d., https://nksc.lrv.lt/lt/naujienos/baltijos-juros-regiono-salyse-dazneja-kibernetines-atakos-nutaikytos-i-kritine-infrastruktura/.
[183] Regional cyber defence centre, „Cyber Threats to Critical Infrastructure in the Baltic Sea Region“, žiūrėta 2026 m. balandžio 4 d., https://www.nksc.lt/doc/rkgc/2024_Cyber_Threats_to_Critical_Infrastructure_in_the_Baltic_Sea_region.pdf.
[184] Nacionalinė kibernetinio saugumo būklės ataskaita 2024, op.cit., 149.
[185] „Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428“, LRS, žiūrėta 2026 m. balandžio 4 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.
[186] *Ibid*.
[187] Europos Komisija, „TIS 2 direktyva: tinklų ir informacinių sistemų apsauga“, žiūrėta 2026 m. balandžio 4 d., https://digital-strategy.ec.europa.eu/lt/policies/nis2-directive.

apimant platesnį ekonomikos veiklų spektrą ir visus sektorius bei paslaugas, kurie yra nepaprastai svarbūs pagrindinei visuomeninei ir ekonominei veiklai, o direktyvos 3 straipsnyje, numatytas naujas kibernetinio saugumo subjektų skirstymas į esminius ir svarbius.[188] Atsižvelgiant į direktyvoje numatytas nuostatas, atnaujinus Kibernetinio saugumo įstatymą, šios nuostatos pradėtos taikyti ir Lietuvoje. Vadovaujantis atnaujinto Kibernetinio saugumo įstatymo **11 straipsnio 1 dalimi**, buvo pradėtas subjektų skirstymas į esminius arba svarbius subjektus kibernetiniam saugumui.[189] Esminiams subjektams yra priskiriamos organizacijos, veikiančios energetikos, transporto, bankininkystės, finansų, sveikatos priežiūros, geriamojo vandens, nuotekų, skaitmeninės infrastruktūros, informacinių ir ryšių technologijų paslaugų valdymo, viešojo administravimo ir kosmoso sektoriuose.[190] Svarbiems subjektams, priskiriamos pašto paslaugų, atliekų tvarkymo, cheminių medžiagų, maisto gamybos, perdirbimo ir platinimo, gamybos, informacinių visuomenės paslaugų, mokslinių tyrimų sektoriuose veikiančios įmonės.[191] Palyginimui, senąjame kibernetinio saugumo įstatyme, kibernetinio saugumo subjektams, buvo priskiriami tik viešojo administravimo subjektai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų arba elektroninių ryšių paslaugų teikėjai, elektroninės informacijos prieglobos paslaugų teikėjai.[192] Verta paminėti ir tai, jog vadovaujantis Kibernetinio saugumo įstatymo **19 straipsnio 1 dalimi**, kibernetinio saugumo subjektų reikalavimus atitinkantys subjektai, turi būti registruojami kibernetinio saugumo subjektų registre.[193] Atnaujinus ir praplėtus kibernetinio saugumo subjektų sąrašą, į minėtą registrą buvo įtrauktos 1443 organizacijos, iš kurių 11 yra esminiai ir 7 svarbūs subjektai. Palyginimui, iki kibernetinio saugumo įstatymo atnaujinimo, ankstesnis registruotų organizacijų skaičius buvo penkis kartus mažesnis.[194] Taigi, išanalizavus Europos Sąjungos Tinklų ir informacinių sistemų direktyva (TIS 2) ir atnaujintą Lietuvos kibernetinio saugumo įstatymą, galime teigti, jog direktyvoje numatytos priemonės, skirtos stiprinti kibernetinį saugumą ir plėsti jo subjektų sąrašą yra tiesiogiai taikomos Lietuvos teisiniame reguliavime.

Atnaujintame Kibernetinio saugumo įstatyme, taip pat buvo įtvirtintos ir baudos už nustatytų reikalavimų nesilaikymą ar trukdymą kibernetinio saugumo politikos įgyvendinimą

---

[188] *Ibid.*
[189] „Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428“, *op.cit.*
[190] Igor Verbickij, „Mažų ir vidutinių organizacijų TIS2 kibernetinio saugumo vertinimo informacinės sistemos projektas“ (magistro baigiamasis darbas, Vilniaus universitetas Šiaulių akademija, 2025), 120-127, https://www.lvb.lt/permalink/370LABT_NETWORK/cdhmhi/alma9919542644408451.
[191] *Ibid, 127-130.*
[192] „2014 m. gruodžio 11 d. Nr. XII-1428 Lietuvos Respublikos kibernetinio saugumo įstatymas“, LRS, žiūrėta balandžio 24 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.
[193] „Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428“, *op.cit.*
[194] „Naujame Lietuvoje kibernetinio saugumo registre – beveik 1500 organizacijų iš 18 sektorių”, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 24 d., https://nksc.lrv.lt/lt/naujienos/naujame-lietuvoje-kibernetinio-saugumo-registre-beveik-1500-organizaciju-is-18-sektoriu/.

atliekančioms institucijoms. 30 straipsnio 2 dalyje, esminiam subjektui numatyta bauda iki 10 mln. eurų, arba iki 2 procentų metinės apyvartos, svarbiam subjektui numatyta iki 7 mln. eurų arba 1,4 procento metinės apyvartos dydžio bauda. Biudžetinei įstaigai, kuri yra esminis subjektas, numatyta iki 1 procento

Siekiant sustiprinti ES šalių bendradarbiavimą kovoje su didelio masto kibernetinėmis atakomis, keliančiomis grėsmė šalių saugumui, bei didinti atsparumą kibernetinėms krizėms, Lietuvos teisėje tiesiogiai taikomas ir 2025 metų vasario 4 d., atnaujintas, **ES Reglamentas 2019/881 (Kibernetinio saugumo aktas)**. Minėtu aktu, siūloma kurti nacionalinius kibernetinio saugumo centrus, kurie, esant poreikiui, galėtų susijungti į tarpvalstybinius kibernetinio saugumo centrus. Centrai atliktų kibernetinių grėsmių stebėjimą, aptikimą ir analizę.[195] Akto 14 straipsnyje taip pat įtvirtintas ir ES kibernetinio saugumo rezervo sukūrimas, kuris sudaromas iš patikimų saugumo paslaugų teikėjų, ir skirtas reaguoti į didelio mąsto, reikšmingus kibernetinio saugumo incidentus.[196]

Kibernetinio saugumo įstatymu, Lietuvoje įgyvendinamas ir **ES Reglamentas 2021/887**, kurio pagrindu Europoje buvo pradėtas plėtoti Nacionalinių koordinavimo centrų tinklas. Nacionaliniai koordinavimo centrai veikia kaip informaciniai centrai nacionaliniu lygmeniu, teikia ekspertines žinias dėl nacionaliniu ir regioniniu lygmeniu kylančių kibernetinio saugumo iššūkių, teikia techninę pagalbą suinteresuotiesiems subjektams ir t.t.[197] Šio ES Reglamento pagrindu, Nacionalinis koordinavimo centras (toliau NKC) savo veiklą 2022 metais veiklą, pradėjo ir Lietuvoje. NKC yra vienas iš 27-ių tokio tipo centrų visoje Europoje, kuris prisideda prie kibernetinio saugumo sistemos stiprinimo ir glaudžiai bendradarbiauja kartu su Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centru (ECCC), įsteigtu Rumunijoje.[198]

Nagrinėjant ES parengtas direktyvas ar reglamentus, svarbu pabrėžti šių dokumentų juridinę galią. Reglamentas yra privalomas, teisėkūros procedūra priimamas aktas ir turi būti taikomas visa apimtimi, visoje ES. Tuo tarpu direktyva yra nustatomi tikslai, kuriuos turi pasiekti ES šalys, tačiau konkretūs įstatymai ir priemones pasiekti tikslui numato pačios valstybės.[199]

---

[195] „Iniciatyvos pagal ES kibernetinio solidarumo aktą“, Lietuvos Respublikos krašto apsaugos ministerija, žiūrėta 2026 m. balandžio 4 d., https://kam.lt/duk/es-kibernetinio-solidarumo-aktas/.

[196] „2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas)“, EUR-Lex, žiūrėta 2026 m. balandžio 6 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A02019R0881-20250204.

[197] Ibid.

[198] „Nacionalinis koordinavimo centras“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 4 d., https://www.nksc.lt/nkc/.

[199] „Teisės aktų rūšys“, Europos Sąjunga, žiūrėta gegužės 4 d., https://european-union.europa.eu/institutions-law-budget/law/types-legislation_lt.

Rūpinantis valstybės saugumu, šalyje taip pat yra parengta **2023-2030 metų Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos pažangos priemonė Nr. 06-007-10-05-07 „Stiprinti kibernetinį atsparumą“.** Parengtos programos 2.1 punkte įtvirtintas *„nacionalinės SOC/CSIRT modulinės sistemos, suteikiančios galimybę SOC/CSIRT paslaugomis naudotis TIS2 direktyvoje nurodytų sektorių kibernetinio saugumo subjektams, sukūrimas“.*[200] Siekiant įgyvendinti minėtą plano punktą, Nacionalinis kibernetinio saugumo centras Lietuvoje pradėjo diegti pažangius kibernetinio saugumo sprendimus kritines paslaugas teikiančiose viešoje sektoriaus įstaigose: ministerijose, savivaldybės įmonėse, vyriausybės įstaigose, valstybės valdomose įmonėse, vandentvarkos asociacijoje, kurios yra pirmose kibernetinės gynybos linijose. Nurodytose organizacijose įsteigus saugumo operacijų centrą (SOC), bus perduodama reikalinga techninė ir programinė įranga, kuri padės užtikrinti greitą reagavimą į kibernetinius incidentus, operatyvų informacijos perdavimą, srauto stebėseną ir pažeidimų šalinimą.[201]

Gerinant pasirengimą elektroninėje erdvėje, šalyje kasmet rengiamos kibernetinio saugumo pratybos. 2024 m. spalio 7-19 d. buvo organizuojamos pratybos **„Kibernetinis Skydas OpEx 2024“**, skirtos viešojo ir privataus sektoriaus organizacijų praktinių įgūdžių stiprinimui, susijusių su reagavimų į kompleksines kibernetines situacijas. Pratybose dalyvavo 80 organizacijų, teikiančių kritines paslaugas Lietuvos gyventojams. Pratybų metu buvo simuliuojamos realios sąlygos, naudojami turimi ištekliai ir procedūros.[202] Tokio tipo pratybos vyko ir 2025 metų lapkričio 17 d., pavadinimu **„Kibernetinis Skydas - TrustEx“.** Šių pratybų metu, didelis dėmesys buvo skiriamas ne vien kritines paslaugas teikiančių organizacijų incidentų valdymo įgūdžiams gerinti, tačiau ir stiprinti tarpusavio bendradarbiavimą ir sąveiką. Pratybose iš viso dalyvavo 28 organizacijos, priklausančios vandentvarkos ir sveikatos priežiūros sektoriams, atsižvelgiant į šių sektorių svarbą nacionaliniam saugumui.[203]

Stiprinant kibernetinį saugumą Lietuvoje, 2025 metais sukurtas naujas Lietuvos kariuomenės junginys – **Kibernetinės gynybos valdyba**. Šios valdybos pagrindinė užduotis stiprinti kariuomenės gynybinius pajėgumus kibernetinėje erdvėje, vykdyti kibernetines

---

[200] „Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos pažangos priemonės Nr. 06-007-10-05-07 „Stiprinti kibernetinį atsparumą “ aprašo patvirtinimo“, TAR, žiūrėta 2026 m. balandžio 4 d., https://www.e-tar.lt/portal/lt/legalAct/5ed44430c3f411eea5a28c81c82193a8.

[201] „Lietuvoje stiprinama pirmoji kibernetinės gynybos linija – steigiami 44 saugumo operacijų centrai“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 6 d., https://nksc.lrv.lt/lt/naujienos/lietuvoje-stiprinama-pirmoji-kibernetines-gynybos-linija-steigiami-44-saugumo-operaciju-centrai-1et/.

[202] „Nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas opex 2024” Ataskaita visuomenei”, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 7 d., https://www.nksc.lt/doc/KS2024_OPEX_Pratybu_ataskaita.pdf.

[203] „Prasidėjo nacionalinės pratybos „Kibernetinis skydas – TrustEx“: sveikatos ir vandentvarkos organizacijos mokosi sektorinės sąveikos“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 7 d., https://www.nksc.lt/naujienos/prasidejo_nacionalines_pratybos_kiberneti_03d18fdf.html.

operacijas, diegti naujas informacines sistemas, taip pat bendradarbiauti su NATO ir kitomis institucijomis kibernetinio saugumo klausimai.[204]

Didelis dėmesys skiriamas ne vien organizacijų, tačiau ir visuomenės švietimo bei atsparumo kibernetinėms grėsmėms, didinimui. 2024 metais NKSC pristatė viešai prieinamą savarankiško mokymosi platformą, kurioje visi norintys gali susipažinti ir įgyti žinių kibernetinio saugumo srityje, dirbtinio intelekto panaudojime. Dalis mokymų skirti ir informacijos saugumo vadovams, saugumo operacijų centro analitikams ir kitiems IT specialistams.[205] NKSC duomenimis, 2025 metais kibernetinio saugumo kursus nuotoliniu būdu išklausė daugiau nei 50 tūkst. gyventojų. Toks skaičius rodo augantį visuomenės poreikį stiprinti kibernetinio saugumo žinias ir praktinius įgūdžius.[206]

Apibendrinant darytina išvada, kad kibernetinės atakos vis dažniau naudojamos kaip netiesioginio poveikio priemonė, kuria siekiama sutrikdyti institucijų veiklą, paveikti visuomenę, skleisti dezinformaciją, mažinti pasitikėjimą valstybe ir kelti nesaugumo jausmą, neperžengiant atviro karinio konflikto ribų. Kibernetinių incidentų mastas ir technologinis sudėtingumas lemia būtinybę nuolat tobulinti tiek teisinį reguliavimą, tiek praktinius valstybės ir visuomenės pasirengimo mechanizmus. Tą rodo kibernetinio saugumo įstatymo atnaujinimas, Europos Sąjungos direktyvos ir reglamentų įgyvendinimas: pradėta Nacionalinio koordinavimo centro veikla, SOC/CSIRT sistemų plėtra. Taip pat reguliariai organizuojamos pratybos ir sukurti viešai prieinami mokymai visuomenei.

[204] „Lietuvos kariuomenės Kibernetinės gynybos valdyba“, Lietuvos Respublikos krašto apsaugos ministerija, žiūrėta 2026 m. balandžio 4 d., https://kam.lt/duk/lietuvos-kariuomenes-kibernetines-gynybos-valdyba/.

[205] „Patogi ir interaktyvi mokymosi platforma“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 7 d., https://www.nksc.lt/mokymai/.

[206] „2025 m. bent vieną NKSC kursą išklausė daugiau nei 50 tūkst. žmonių“, Nacionalinis kibernetinio saugumo centras, žiūrėta 2026 m. balandžio 7 d., https://www.nksc.lt/naujienos/2025_m_bent_viena_nksc_kursa_isklause_dau_76d90086.html.

IŠVADOS

1. Atlikus mokslinių straipsnių, nagrinėjusių hibridinių grėsmių reiškinį, analizę nustatyta, kad hibridinių grėsmių terminas yra pakankamai naujas ir pirmą kartą buvo paminėtas 2007 metais. Hibridinių grėsmių samprata yra sunkiai apibrėžiama dėl nuolat vykstančių technologinių, geopolitinių ir kitų pasikeitimų, tačiau sutinkama, kad tai yra prievartinių ir ardomųjų veiklų, konvencinių ir nekonvencinių metodų derinys, naudojamas valstybinių ar nevalstybinių subjektų, siekiančių priešiškų tikslų, neskelbiant karo ir išliekant žemiau oficialaus karo ribos. Šiomis priemonėmis siekiama destabilizuoti padėtį valstybėje, sukelti visuomenes abejones valstybinių institucijų darbu, didinti nesaugumo jausmą. Į hibridinės grėsmės sąvoką patenka karinių ir nekarinių priemonių, tokių kaip diplomatinis, ekonominis spaudimas, kibernetiniai išpuoliai, dezinformacija panaudojimas. Identifikuoti kylančias grėsmės ir jų šaltinį ypač sudėtinga dėl subjektų veikimo „pilkojoje zonoje“, neaiškaus priešo buvimo ir oficialaus karo nepaskelbimo.
2. Nacionalinis šalies saugumas yra suprantamas, kaip valstybės teritorijos, suvereniteto ir jos gyventojų apsauga nuo išorinių ir vidinių grėsmių. Nacionalinio saugumo užtikrinimas susideda iš tikslingų ir kryptingų visuomenės ar valstybės veiksmų, kurių pagrindinis tikslas - užtikrinti valstybės suverenitetą, konstitucinę tvarką, vystyti gerovės valstybę. Tai yra prioritetinė valstybės ir jos institucijų veiklos sritis, reikalaujanti ypatingo dėmesio, išteklių ir nuoseklios, ilgalaikės strategijos, teisinio reguliavimo pakeitimų. Nacionaliniam saugumui įtaką daro aplinkosaugos, kariniam, ekonominiam, kibernetiniam, socialiniam ar politiniam valstybės sektoriams kylančios grėsmės. Pastarųjų metų įvykiai: „Ikea“ padegimas, savaime užsidegančios siuntos ir kt. parodė, kad Lietuva susiduria su Rusijos ir Baltarusijos vykdomais hibridiniais išpuoliais ir tai tiesiogiai veikia šalies nacionalinį saugumą.
3. Atsižvelgiant į hibridinių grėsmių sudėtingumą, ankščiau taikytos saugumo priemonės ir reagavimo algoritmai į hibridines grėsmes ES šalyse tampa neveiksmingi, todėl kyla būtinybė ieškoti vis naujų priemonių ir sprendimo būdų. Hibridinių grėsmių poveikis įvairiems valstybės sektoriams rodo, kad nė viena valstybė savarankiškai negali užtikrinti efektyvaus atsako į tokio pobūdžio grėsmes. Atsižvelgiant į tai, Europos Sąjunga ir NATO vykdo kryptingą ir nuoseklų darbą hibridinių grėsmių prevencijos ir kovos srityje. ES parengti veiksmų planai, strategijos ir kiti dokumentai rodo, jog hibridinių grėsmių keliami pavojai ir toliau išlieka prioritetiniu Europos Sąjungos klausimu saugumo srityje. Kovoje su hibridinėmis grėsmėmis, ES akcentuoja kibernetinį, ypatingos svarbos infrastruktūros saugumą, valstybių narių tarpusavio bendradarbiavimą, prevencinių ir atsakomųjų veiksmų koordinuotumą, bendradarbiavimą su sąjungininkais, tarp jų ir NATO. ES ir NATO partnerystė hibridinių grėsmių kontekste palaipsniui pereina nuo tradicinio politinio bendradarbiavimo modelio į visapusišką strateginio saugumo sistemą: NATO užtikrina kolektyvinę gynybą, atgrasymą ir reagavimą, o Europos Sąjunga kuria

teisėkūros, reguliavimo ir vidaus atsparumo stiprinimo priemones. Šių dviejų organizacijų bendradarbiavimas nuosekliai stiprėja ir įgauna vis didesnę praktinę reikšmę per bendras deklaracijas, koordinuotas pratybas, informacijos mainus, kritinės infrastruktūros apsaugos iniciatyvas bei paramos mechanizmus valstybėms narėms.

4. Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas ir Lietuvos nacionalinio saugumo strategija yra pagrindiniai teisės aktai, apibrėžiantys nacionalinio saugumo suvokimą Lietuvoje, nustatantys pagrindinius interesus, prioritetus ir uždavinius šalies nacionalinio saugumo srityje. Dėl hibridinių grėsmių daugialypiškumo, buvusių saugumo priemonių ir mechanizmų nebeužtenka, todėl valstybės nacionalinio saugumo politika keičiasi, pereidama nuo prevencijos, prie visuotinio saugumo ir gynybos stiprinimo. Įgyvendinant nacionalinio saugumo strategijos tikslus, valstybė imasi aktyvių priemonių kovojant su iškilusiomis hibridinėmis grėsmėmis: priimtas naujas Krizių valdymo ir civilinės saugos įstatymas, įkurtas Nacionalinis krizių valdymo centras, patvirtinta Civilinės saugos stiprinimo ir plėtros programa, gyventojai šviečiami hibridinių grėsmių ir pilietinio pasipriešinimo srityje, organizuojamos bendros valstybinių institucijų pratybos kritinės infrastruktūros apsaugos srityje.
5. Atlikus meteorologinių balionų atvejo analizę nustatyta, kad naudojimas gabenant akcizais apmokestinamas prekes iš Baltarusijos į Lietuvą peržengė tradicinės kontrabandos ribas, įgijo hibridinių grėsmių pobūdį ir tapo tikru iššūkiu Lietuvos nacionaliniam saugumui. Lietuvos valstybės atsakas į šią grėsmę yra kompleksinis, apimantis tiek teisės aktų pakeitimus, tiek ir krizių valdymo, tarpinstitucinio bendradarbiavimo, bei kitų priemonių įgyvendinimo visumą: LR Baudžiamojo kodekso straipsniai, susije su kontrabanda, buvo papildyti naujomis kvalifikuotomis nusikalstamų veikų sudėtimis, LR Baudžiamojo kodekso 118 straipsnis buvo papildytas naujomis dalimis, susijusiomis su padėjimu veikti prieš valstybę, to paties straipsnio 1 dalies sankcija buvo sugriežtinta, įtraukta nauja kvalifikuojanti, veikos pavojingumą didinanti, sudėtis, LR Kriminalinės žvalgybos įstatymo 8 straipsnio 1 dalies 1 punktas papildytas LR Baudžiamojo kodekso 282 straipsnio 2 dalyje numatyta nusikalstama veika, valstybėje paskelbta ekstremalioji situacija, praplėsti karių įgaliojimai, išplėstos statutinių pareigūnų teisės panaudoti šaunamąjį ginklą ar sprogmenis prieš autonomiškai arba nuotoliniu būdu valdomą objektą, pradėti bendri policijos, VSAT, Karo policijos ir kitų institucijų reidai pasienio ruožuose. Atlikti pakeitimai rodo, jog teisinis reguliavimas turi prisitaikyti prie kylančių grėsmių, ir šiai dienai nėra pakankamas. Atsakas į hibridines grėsmes reikalauja priemonių visumos, todėl reaguojant į šią iškilusią grėsmę ir ieškant sprendimo būdų, į procesą yra įtraukiamas ir verslas, ir pati visuomenė.
6. Atlikus baigiamojo darbo antrojo atvejo – kibernetinių išpuolių analizę nustatyta, kad kibernetinės atakos vis dažniau naudojamos kaip netiesioginio poveikio priemonė, kuria siekiama sutrikdyti institucijų veiklą, paveikti visuomenę, skleisti dezinformaciją, mažinti pasitikėjimą valstybe ir

kelti nesaugumo jausmą, neperžengiant atviro karinio konflikto ribų. Lietuvos atsakas į kibernetines grėsmes yra nuoseklus ir sisteminis. Kibernetinių incidentų mastas ir technologinis sudėtingumas lemia būtinybę nuolat tobulinti tiek teisinį reguliavimą, tiek praktinius valstybės ir visuomenės pasirengimo mechanizmus. Tą rodo kibernetinio saugumo įstatymo atnaujinimas, kuriuo Lietuvos teisinėje sistemoje pradėta įgyvendinta ES direktyva TIS2, išplėstas kibernetinio saugumo subjektų ratas, sugriežtinta atsakomybė, piniginės baudos už kibernetinio saugumo pažeidimus. Taip pat visa apimtimi pradėtas taikyti ES Reglamentas 2019/881 (Kibernetinio saugumo aktas), ir ES Reglamentas 2021/887, kurio pagrindu Lietuvoje pradėjo veikti Nacionalinio koordinavimo centras, pradėta SOC/CSIRT sistemų plėtra. Kibernetiniam saugumui užtikrinti reguliariai organizuojamos bendros pratybos: „Kibernetinis Skydas OpEx 2024“, „Kibernetinis Skydas - TrustEx“, sukurtas naujas Lietuvos kariuomenės junginys – Kibernetinės gynybos valdyba, sukurti viešai prieinami mokymai visuomenei apie kibernetinį saugumą.

LITERATŪROS SĄRAŠAS

Teisės aktai:

1. „Visuotinė žmogaus teisių deklaracija“. LRS. Žiūrėta 2022 m. gruodžio 17 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385.
2. „Europos Žmogaus teisių konvencija“. Žiūrėta 2025 m. lapkričio 8 d. https://www.echr.coe.int/documents/d/echr/convention_lit.
3. „2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas)“. EUR-Lex. Žiūrėta 2026 m. balandžio 6 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A02019R0881-20250204.
4. Europos Komisija. „TIS 2 direktyva: tinklų ir informacinių sistemų apsauga“. Žiūrėta 2026 m. balandžio 4 d. https://digital-strategy.ec.europa.eu/lt/policies/nis2-directive.
5. „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“. TAR. Žiūrėta 2026 m. vasario 26 d. https://www.e-tar.lt/portal/lt/legalAct/TAR.A0BAB27D768C/hlQneKjoWb.
6. „Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas“. TAR. Žiūrėta 2026 m. kovo 24 d. https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr?csrt=7351734137272631161.
7. „2000 m. rugsėjo 26 d. Nr. VIII-1968 Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas“. TAR. Žiūrėta 2026 m. balandžio 20 d. https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/wZXqTUOQzz.
8. „2014 m. gruodžio 11 d. Nr. XII-1428 Lietuvos Respublikos kibernetinio saugumo įstatymas“. LRS. Žiūrėta balandžio 24 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.
9. „Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428“. LRS. Žiūrėta 2026 m. balandžio 4 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.
10. „Lietuvos Respublikos policijos įstatymas“. TAR. Žiūrėta 2026 m. kovo 25 d. https://www.etar.lt/portal/lt/legalAct/TAR.CA89372D00AA/GQPVYLUSox?csrt=1320035902353116754.

11. „Lietuvos Respublikos aviacijos įstatymo Nr. VIII-2066 2 ir 18 straipsnių pakeitimo įstatymas“. TAR. Žiūrėta 2026 m. balandžio 15 d. https://www.e-tar.lt/portal/lt/legalAct/dac62e32a8b611ef90b5ee8931e5ce5e.
12. „Lietuvos Respublikos baudžiamojo kodekso 114, 118, 119, 120 ir 121 straipsnių pakeitimo įstatymas”. TAR. Žiūrėta 2026 m. balandžio 20 d. https://www.e-tar.lt/portal/lt/legalAct/8e1931e0299011efbdaea558de59136c.
13. „Lietuvos Respublikos baudžiamojo kodekso 9-1, 118 ir 119 straipsnių pakeitimo įstatymas“. TAR. Žiūrėta 2026 m. balandžio 20 d. https://e-tar.lt/portal/lt/legalAct/7bfd8700e1ac11ec8d9390588bf2de65.
14. „Lietuvos Respublikos kriminalinės žvalgybos įstatymo Nr. XI-2234 8 straipsnio pakeitimo įstatymas“. TAR. Žiūrėta 2026 m. kovo 25 d. https://www.e-tar.lt/portal/lt/legalAct/bb385fe0d9b411f08918e1adc7c5b1ec?csrt=17509282981660083539.
15. „Lietuvos Respublikos policijos įstatymo Nr. VIII-2048 2, 27 ir 28 straipsnių pakeitimo įstatymas“. TAR. Žiūrėta 2026 m. kovo 25 d. https://www.e-tar.lt/portal/lt/legalAct/59aaf352a8b411ef90b5ee8931e5ce5e?csrt=13200359023531167 54.
16. „Dėl Nacionalinio saugumo strategijos patvirtinimo”. TAR. Žiūrėta 2026 m. sausio 19 d. https://www.e-tar.lt/portal/tt/legalAct/TAR.2627131DA3D2/asr.
17. „Nutarimas „Dėl Lietuvos Respublikos baudžiamojo kodekso 199, 199^2, 253^2, 256^2, 260^1, 266^1, 267^2, 267^3, 276^4 ir 282^1 straipsnių pakeitimo įstatymo, Lietuvos Respublikos kriminalinės žvalgybos įstatymo 8 straipsnio pakeitimo įstatymo projektų pateikimo“. TAR. Žiūrėta 2026 m. kovo 23 d. https://www.e-tar.lt/portal/lt/legalAct/d26f05b0c0aa11f092fda1fd0c194cc5.
18. „Nutarimas „Dėl teisių kariams suteikimo ekstremaliosios situacijos atveju“. TAR. Žiūrėta 2026 m. kovo 3 d. https://www.e-tar.lt/portal/lt/legalAct/404b5fa2dc1911f08918e1adc7c5b1ec.
19. „Nutarimas „Dėl valstybės lygio ekstremaliosios situacijos paskelbimo ir valstybės lygio ekstremaliosios situacijos valstybės operacijų vadovo paskyrimo“. TAR. Žiūrėta 2026 m. kovo 3 d. https://www.e-tar.lt/portal/lt/legalAct/603808e2d4cb11f08918e1adc7c5b1ec.
20. „Nutarimas „Dėl civilinės saugos stiprinimo ir plėtros programos patvirtinimo“. TAR. Žiūrėta 2026 m. kovo 23 d. https://e-tar.lt/portal/lt/legalAct/74b9f360459211efbdaea558de59136c.

21. „Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos pažangos priemonės Nr. 06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ aprašo patvirtinimo“. TAR. Žiūrėta 2026 m. balandžio 4 d. https://www.e-tar.lt/portal/lt/legalAct/5ed44430c3f411eea5a28c81c82193a8.
22. „Aiškinamasis raštas „Dėl Lietuvos Respublikos baudžiamojo kodekso 199, 199^2, 253^2, 256^2, 260^1, 266^1, 267^2, 267^3, 276^4 ir 282 straipsnių pakeitimo įstatymo, Lietuvos Respublikos kriminalinės žvalgybos įstatymo 8 straipsnio pakeitimo įstatymo projektų“. TAR. Žiūrėta 2026 m. kovo 23 d. https://www.e-tar.lt/rs/lasupplement/d26f05b0c0aa11f092fda1fd0c194cc5/ff72aa89c0af11f092fda1fd0c194cc5/format/ISO_PDF/?csrt=10097897341412856574.

Moksliniai šaltiniai:

1. AI Aridi, Alaa AI Dakour. „Hibridinio karo problema tarpautinėje teisėje”. Daktaro disertacija, Vilniaus universitetas, 2022. https://epublications.vu.lt/object/elaba:149038012.
2. Alaburdaitė, Ugnė. „Hibridinių grėsmių prevencijos teisinė sistema“. Magistro baigiamasis darbas, Mykolo Romerio universitetas, 2025. https://www.lvb.lt/permalink/370LABT_NETWORK/cdhmhi/alma9917024127908451
3. Almäng, Jan. „War, Vagueness and Hybrid War“. Defence Studies 19, 2 (2019): 193.https://www.tandfonline.com/doi/epdf/10.1080/14702436.2019.1597631?needAccess=true.
4. Bachmann, Sascha-Dominik. „Hybrid threats, cyber warfare and NATO comprehensive approach for countering 21 st. Century threats – mapping the new frontier of global riskand the security management“. Amicus Curiae 88, 2012: 17. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989808.
5. Bajarūnas, Eitvydas. *„Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond“*. European View 19, 1 (2020): 62. https://doi.org/10.1177/1781685820912041.
6. Bertašienė, Aušra. „Lietuvos nacionalinio saugumo rizikos veiksniai ir jų valdymas“. Magistro baigiamasis darbas, Klaipėdos universitetas, 2025. https://portalcris.ku.lt/server/api/core/bitstreams/7d235b4f-b380-4f35-9d6f-54b026ae89cb/content.

7. Cirdei, Ionut Alin, Lucian Ispas. „A possible answer of the European Union to hybrid threats". *Buletin stiintific*, 2, 44 (2017): 72. https://www.armyacademy.ro/buletin/bul2_2017/CARDEI.pdf.
8. Estevens, Joao. „Migration crisis in the EU: developing a framework for analysis of national security and defence strategies", *Estevens Comparative Migration Studie* 6, 28 (2018): 3. https://link.springer.com/article/10.1186/s40878-018-0093-3.
9. Fjader, Christian. „The nation-state, national security and resilience in the age of globalisation". *Resilience* 2, 2 (2014): 117. https://doi.org/10.1080/21693293.2014.914771.
10. Giannopoulos, Georgios, Hanna Smith ir Marianthi Theocharidou. „The landscape of Hybrid Threats: A conceptual model". *European Union and Hybrid CoE*, (2021): 6. https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.
11. Greičius, Saulius, Birutė Pranevičienė. „Asmens ir valstybės saugumo samprata, užtikrinimo poreikis ir problemos". *Regnum est: 1990 m. Kovo 11-osios nepriklausomybės Aktui-20: Liber Amicorum Vytautui Landsbergiui,* 2010: 722. https://cris.mruni.eu/server/api/core/bitstreams/838726e2-7251-4e09-b912-35402bb5652b/content.
12. Hindren, Rasmus. *Hybrid threats and the EU's Strategic Compass*. Helsinkis: European Centre of Excellence for Countering Hybrid Threats, 2021. https://www.hybridcoe.fi/wp-content/uploads/2021/10/Hybrid_CoE_Working_Paper_12_Calibrating_the_compass_WEB.pdf.
13. Hoffman, G. Frank. „Conflict in the 21st century: the rise of hybrid war". Potomac Institute for Policy Studies, 2007. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
14. Isoda, Vytautas. „Visuomenės ontologinio saugumo samprata: Lietuvos nacionalinio saugumo ontologinė dimensija". *Visuomenės saugumas ir viešoji tvarka* 18 (2017): 8. https://ojs.mruni.eu/ojs/vsvt/article/view/5618/4825.
15. Kaplan, Alan Mitchell. „The Socioeconomic and Political Ramifications of Climate Migration in the 21st Century". IGI Global Scientific Publishing, 2024. https://www.researchgate.net/publication/359882823_The_Socioeconomic_and_Political_Ramifications_of_Climate_Migration_in_the_21st_Century.

16. Karpavičiūtė, Ieva. „Securitization and Lithuania's National Security Change". *Lithuanian Foreign Policy Review* 36 (2017): 10. https://doi.org/10.1515/lfpr-2017-0005.
17. Kazlauskaitė-Markelienė, Rolanda, Audronė Petrauskaitė. „Pilietinė visuomenė ir nacionalinis saugumas: teorine problemos apžvalga". *Generolo Jono Žemaičio Lietuvos karo akademija* 9, 1 (2011): 237. https://doi.org/10.47459/lmsa.2011.9.11.
18. Keršanskas, Vytautas. „Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats". The European Centre of Excellence for Countering Hybrit Threats, 2020: 8. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.
19. Lasoen, Kenneth. „Realising the EU Hybrid Toolbox: opportunities and pitfalls". Clingendael. Žiūrėta 2026 m. vasario 16 d. https://www.clingendael.org/sites/default/files/202212/Policy_brief_EU_Hybrid_Toolbox.pdf.
20. Leibenka, Vitalijus. „Ketvirtosios kartos karas", Kultūros barai 10, (2019): 2-7. https://etalpykla.lituanistika.lt/object/LT-LDB0001:J.04~2018~1615394203071/J.04~2018~1615394203071.pdf.
21. Mälksoo, Maria. „Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO". European Security 27, 3 (2018): 12. https://doi.org/10.1080/09662839.2018.1497984.
22. Matonytė, Irmina, Ieva Gajauskaitė ir Matas Jasinavičius. „Hibridinės grėsmės Lietuvoje: sampratos žinomumas ir raiškos formų atpažinimas jaunimo tarpe". Viešoji politika ir administravimas 23, 3 (2024): 357. https://doi.org/10.5755/j01.ppaa.23.3.35169.
23. Mockaitis, R. Thomas. „Conventional and Unconventional War – A history of Conflict in the Modern World". Bloomsbury Publishing USA, 2017.
24. Monboe Nebo, Ambrues. „National Security Strategy: A Toolkit for Assessing State Preparedness to Combat Global Security Threats That Endanger National Security in the 21st Century", *ISRG Journal of Arts Humanities & Social Sciences* 2, 5 (2024): 396. https://doi.org/10.5281/zenodo.13953887.
25. Monoghan, Sean. „Countering Hybrid Warfare", *Features* 8, 2, (2019): 86. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf?ver=2019-09-17-231051-890.
26. Monoghan, Sean. „Countering Hybrid Warfare". 2019. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf?ver=2019-09-17-231051-890.

27. Nastavičienė, Justina. „Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje įtvirtintų įmonių teisių apsaugos problemos ES konkurencijos teisėje“. Daktaro disertacija. Mykolo Romerio universitetas, 2012. https://cris.mruni.eu/server/api/core/bitstreams/ce515261-4e3e-4004-b97a-c56067957c37/content.
28. Nevera, Andrius. „2025 m. Baudžiamojo kodekso pokyčiai ir jų vertinimas“.Lietuvos teisė 2025: esminiai pokyčiai. Vilnius: Mykolo Romerio universitetas, 2025. https://cris.mruni.eu/cris/handle/007/50581.
29. Petrauskaitė, Asta, Rasa Kazlauskaitė-Markelienė ir Rasa Gedminienė. *Šalies saugumas ir gynyba: metodinė medžiaga Lietuvos bendrojo lavinimo mokyklų mokytojams*. Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2016. https://biblioteka.lka.lt/data/Leidiniai/sisteminis_katalogas/Informaciniai-reprezentaciniai/2016-salies saugumas ir gynyba-metodine.pdf.
30. Racz, Andras. „Russia‘s Hybrid War in Ukraine: breaking the enemy‘s ability to resist“. The Finnish institute of international affairs, 2015. https://fiia.fi/en/publication/russias-hybrid-war-in-ukraine.
31. Renz, Bettina. „Russia and ‘hybrid warfare’”. Contemporary Politics 22, 3 (2016): 283. https://doi.org/10.1080/13569775.2016.1201316.
32. Sanz-Caballero, Susana. „The concepts and laws applicable to hybrid threats, with a special focus on Europe“. *Humanities and Social Sciences Communications*, 10, 360 (2023): 2. https://doi.org/10.1057/s41599-023-01864-y.
33. Sari, Aurel. „Hybrid threats and the law: Building legal resilience”. Hybrid CoE Research, Report 3 (2021): 19. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-3-hybrid-threats-and-the-law-building-legal-resilience/.
34. Seniutienė, Danguolė, Laima Paulauskytė. „Response to Hybrid Threats: Policies, Concepts and Strategic Approaches“. Public Security and Public Order 36 (2024): 195–202. https://doi.org/10.13165/PSPO-24-36-14.
35. Štareikė, Eglė. „Countering Hybrid Threats: Problematic Aspects in the European Region”. Public Security and Public Order, 36, (2024): 229. https://doi.org/10.13165/PSPO-24-36-17.
36. Summers, James. „The Crimea Crisis: A Case of Occupation, Annexation, Secession or Autonomy?“. Lancaster university law school. Žiūrėta 2025 m. lapkričio 8 d. https://lancslaw.wordpress.com/2014/03/05/the-crimea-crisis/.
37. Sykulski, Leszek. „Old Methods in the New Framework”. Strategy of Grey Zones in Hybrid Warfare, Strategies XXI – National Defence College”. *Proceedings 2021*

„Romania and the new dynamics of international security" 1, 72 (2021): 163. https://doi.org/10.53477/2668-5094-21-11.

38. Tidikis, Rimantas. *Socialinių mokslų tyrimų metodologija*. Vilnius: Lietuvos teisės universitetas, 2003.
39. Tropin, Zakhar. „Lawfare as part of hybrid wars: The experience of Ukraine in conflict with Russian Federation". Security and Defence Quarterly, 2021. https://doi.org/10.35467/sdq/132025.
40. Verbickij, Igor. „Mažų ir vidutinių organizacijų TIS2 kibernetinio saugumo vertinimo informacinės sistemos projektas". Magistro baigiamasis darbas, Vilniaus universitetas Šiaulių akademija, 2025. https://www.lvb.lt/permalink/370LABT_NETWORK/cdhmhi/alma991954264440845.
41. Weissmann, Mikael. „Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework". Journal on Baltic Security, 5, 1 (2019): 2. https://www.researchgate.net/publication/334967002_Hybrid_warfare_and_hybrid_threats_today_and_tomorrow_towards_an_analytical_framework.
42. Wyrebek, Henryk. „National security challanges and threats", *Wiedza Obronna* 279, 2 (2022): 2. https://doi.org/10.34752/2022-e279.

Specialioji literatūra:

1. „Nacionalinė kibernetinio saugumo būklės ataskaita: pernai 63 proc. išaugo kibernetinių incidentų skaičius". Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 4 d. https://www.nksc.lt/naujienos/nacionaline_kibernetinio_saugumo_bukles_ataskaita_.html.
2. „Nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas opex 2024" Ataskaita visuomenei". Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 7 d. https://www.nksc.lt/doc/KS2024_OPEX_Pratybu_ataskaita.pdf.
3. *„ProtectEU" – Europos vidaus saugumo strategija*". Europos Komisija (COM(2025) 148 final). Žiūrėta 2026 m. vasario 16 d. https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A52025DC0148.
4. *2025 metų veiklos ataskaita*. Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. Vilnius, 2026. https://vsat.lrv.lt/public/canonical/1773657041/6190/2025%20m.%20VSAT%20veiklos%20ataskaita.pdf.

5. Bajarūnas, Eitvydas, Vytautas Keršanskas. „Hibridinės grėsmės: turinio, keliamų iššūkių ir priemonių įveikti jas analizė". *Lietuvos metinė strateginė apžvalga*, 16, (2017-2018): 128. https://kam.lt/wp-content/uploads/2023/01/Bajarunas-Kersanskas.-Hibridines-gresmes-turinio-keliamu-issukiu-ir-priemoniu-iveikti-jas-analize.-Metine-strategine-apzvalga-LKA-2017-2018.pdf.
6. Bileišis, Mantas, Svajūnė Ungurytė-Ragauskienė. „Nacionalinio saugumo iššūkiai: viešojo valdymo tobulinimo aktualijos", iš Saugumo iššūkiai: Vadybos tobulinimas: Kolektyvinė monografija, 16-35. Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2020. https://vb.lka.lt/object/elaba:89853199/89853199.pdf.
7. Costa, Rita. *Hybrid threats in the context of European security*. National Defense Institute of Portugal, 2022. https://comum.rcaap.pt/bitstream/10400.26/37389/1/COSTARita_Hybridthreatsincontextofeuropeansecurity_E_BriefinsPapers_Maio_2021.pdf.
8. Council of the European Union. „Food-for-thought paper „Countering hybrid Threats". Žiūrėta 2026 m. sausio 25 d. https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf.
9. European Commision. Joint communication to the european parliamant and the council. Joint Framework on contering hybrid threats (JOIN(2016) 18 final, 2016 m. birželio 4 d.). Žiūrėta 2026 m. sausio 25 d. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52016JC0018.
10. European Union External Action Service. „*A Strategic Compass for Security and Defence*". Žiūrėta 2026 m. vasario 11 d. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.
11. Europos Komisija. „Bendras komunikatas Europos Parlamentui ir Tarybai. Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas". Žiūrėta 2025 m. lapkričio 15 d. http://eur-lex.europa.eu/ legal-content/LT/TXT/?uri=CELEX%3A52016JC0018.
12. Europos Komisija. „Bendras komunikatas Europos Parlamentui ir Tarybai. Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas". Žiūrėta 2025 m. lapkričio 15 d. http://eur-lex.europa.eu/ legal-content/LT/TXT/?uri=CELEX%3A52016JC0018.
13. Europos Komisija. *Atsparumo didinimas ir kovos su hibridinėmis grėsmėmis pajėgumų plėtra. Bendras komunikatas* (JOIN(2018) 16 final, 2018 m. birželio 13 d.). Žiūrėta 2026

m. vasario 11 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52018JC0016.

14. Europos Sąjunga. „EU Preparedness Union Strategy". Europos Sąjungos leidinių biuras. Žiūrėta 2026 m. vasario 16 d. https://commission.europa.eu/topics/preparedness_en.
15. Europos Sąjungos Taryba. Tarybos išvados dėl pagrindo koordinuotam ES atsakui į hibridines kompanijas. Žiūrėta 2026 m. vasario 11 d. https://data.consilium.europa.eu/doc/document/ST-10016-2022-INIT/lt/pdf.
16. Europos Vadovų Taryba. „Strategic Agenda 2024–2029". Žiūrėta 2026 m. vasario 16 d. https://www.consilium.europa.eu/media/yxrc05pz/sn02167en24_web.pdf.
17. *Grėsmių nacionaliniam saugumui vertinimas.* Valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. Vilnius, 2026. https://www.vsd.lt/wp-content/uploads/2026/03/2026-GR-LT-El_NAUJAS.pdf.
18. Janeliūnas, Tomas, Laura Kirvelytė. „Gruzijos saugumo strategijos plėtra: sunkus kelias NATO link". Lietuvos metinė strateginė apžvalga 7, 1 (2009): 149-151. https://journals.lka.lt/journal/lmsa/article/1764/info.
19. Lietuvos Respublikos krašto apsaugos ministerija. „Atnaujintas kibernetinio saugumo įstatymas". Žiūrėta 2026 m. balandžio 4 d. https://kam.lt/wp-content/uploads/2024/10/Atnaujintas-kibernetinio-saugumo-istatymas.pdf.
20. Lietuvos Respublikos krašto apsaugos ministerija. *Lietuvos kibernetinio saugumo būklės apžvalga: svarbiausia informacija 2024*. Žiūrėta 2026 m. balandžio 4 d. https://kam.lt/wp-content/uploads/2025/07/Nacionalines-kibernetinio-saugumo-bukles-ataskaitos-santrauka-2024.pdf.
21. Lietuvos Respublikos krašto apsaugos ministerija. *Nacionalinė kibernetinio saugumo būklės ataskaita 2022.* Vilnius, 2022. https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf.
22. Lietuvos Respublikos krašto apsaugos ministerija. *Nacionalinė kibernetinio saugumo būklės ataskaita 2024.* Vilnius, 2025. https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2024.pdf.
23. Matonytė, Irmina, Ieva Gajauskaitė ir Viktor Denisenko. *Hibridinės grėsmės: nuo neapibrėžtumo iki atsparumo*. Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija, 2025. https://portalcris.vdu.lt/server/api/core/bitstreams/fe7ffc81-242f-468c-ad96-d175e681ae2e/content.
24. Pawlak, Patryk. „Understanding hybrid threats". European Parliament. Žiūrėta 2025 m. lapkričio 14 d. https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/.
25. Regional cyber defence centre. „Cyber Threats to Critical Infrastructure in the Baltic Sea Region". Žiūrėta 2026 m. balandžio 4 d.

https://www.nksc.lt/doc/rkgc/2024_Cyber_Threats_to_Critical_Infrastructure_in_the_Baltic_Sea_region.pdf.

Internetiniai šaltiniai:

1. „„ProtectEU“. Komisija pristato naują kovos su terorizmu darbotvarkę“. Europos Komisija. Žiūrėta 2026 m. gegužės 4 d. https://ec.europa.eu/commission/presscorner/detail/lt/ip_26_423.
2. „2025 m. bent vieną NKSC kursą išklausė daugiau nei 50 tūkst. žmonių“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 7 d. https://www.nksc.lt/naujienos/2025_m_bent_viena_nksc_kursa_isklause_dau_76d90086.html.
3. „Antradienį perimtos 7 iš Baltarusijos oro balionais skraidintos rūkalų siuntos (video)“. Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. Žiūrėta 2026 m. kovo 23 d. https://vsat.lrv.lt/lt/naujienos/antradieni-perimtos-7-is-baltarusijos-oro-balionais-skraidintos-rukalu-siuntos-video-bfc.
4. „Baltijos jūros regiono šalyse dažnėja kibernetinės atakos nutaikytos į kritinę infrastruktūrą“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 4 d. https://nksc.lrv.lt/lt/naujienos/baltijos-juros-regiono-salyse-dazneja-kibernetines-atakos-nutaikytos-i-kritine-infrastruktura/.
5. „Bartkus patikino: daugiau aviakompanijų keisti krypčių dėl balionų neplanuoja“. Lietuvos nacionalinis radijas ir televizija. Žiūrėta 2026 m. kovo 23 d. https://www.lrt.lt/naujienos/verslas/4/2773256/bartkus-patikino-daugiau-aviakompaniju-keisti-krypciu-del-balionu-neplanuoja?srsltid=AfmBOopxqEGUIm6MGJUfGJbUdqsBohYKqiPxyMWfH-xCsB84r652jSoE.
6. „Brussels Summit Declaration“. NATO. Žiūrėta 2026 m. vasario 20 d. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2018/07/11/brussels-summit-declaration.
7. „Countering hybrid threats“. NATO. Žiūrėta 2026 m. vasario 20 d. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.
8. „Dėl Lietuvos Respublikos Vyriausybės kanclerio 2023 m. sausio 19 d. įsakymo Nr. V-15 „Dėl Lietuvos Respublikos Vyriausybės kanceliarijos 2023–2025 metų strateginio veiklos plano patvirtinimo“ pakeitimo“. Lietuvos Respublikos Vyriausybė. Žiūrėta 2026 m. vasario 27 d. https://lrv.lt/media/viesa/saugykla/2023/12/9KvAXF0cYHk.pdf.

9. „Dėl suintensyvėjusios Baltarusijos hibridinės atakos Lietuva ragina ES imtis ryžtingų priemonių“. Lietuvos Respublikos vidaus reikalų ministerija. Žiūrėta 2026 m. kovo 2 d. https://vrm.lrv.lt/lt/naujienos/del-suintensyvejusios-baltarusijos-hibridines-atakos-lietuva-ragina-es-imtis-ryztingu-priemoniu-M9rX/.
10. „EIMIN skelbia iki 1 mln. eurų vertės programą – siekia greitų technologinių sprendimų oro erdvės saugumui“. Lietuvos Respublikos ekonomikos ir inovacijų ministerija. Žiūrėta 2026 m. balandžio 8 d. https://eimin.lrv.lt/lt/ziniasklaidai/naujienos/eimin-skelbia-iki-1-mln-euru-vertes-programa-siekia-greitu-technologiniu-sprendimu-oro-erdves-saugumui-Q0XR/.
11. „Europos Sąjungos parengties strategija: koordinuotas atsakas į šių dienų grėsmes“. Lietuvos Respublikos vidaus reikalų ministerija. Žiūrėta 2026 m. vasario 16 d. https://vrm.lrv.lt/lt/naujienos/europos-sajungos-parengties-strategija-koordinuotas-atsakas-i-siu-dienu-gresmes/.
12. „Hibridinė Baltarusijos ataka prieš Lietuvą“. Lietuvos Respublikos Vyriausybė. Žiūrėta 2026 m. kovo 23 d. https://lrv.lt/lt/hibridine-baltarusijos-ataka-pries-lietuva.
13. „Hibridinėms grėsmėms – vieningas VRM tarnybų atsakas“. Lietuvos Respublikos vidaus reikalų ministerija. Žiūrėta 2026 m. vasario 27 d. https://vrm.lrv.lt/lt/naujienos/hibridinems-gresmems-vieningas-vrm-tarnybu-atsakas.
14. „Į Lietuvą atvyko NATO kovos su hibridinėmis grėsmėmis ekspertų komanda”. Lietuvos Respublikos Krašto apsaugos ministerija. Žiūrėta 2025 m. lapkričio 15 d. https://kam.lt/i-lietuva-atvyko-nato-kovos-su-hibridinemis-gresmemis-ekspertu-komanda/.
15. „Ikea“ padegimo byla: kruopščiai rengtas tarptautinis Rusijos teroro aktas“. Delfi. Žiūrėta 2026 m. sausio 19 d. https://www.delfi.lt/news/daily/lithuania/ikea-padegimo-byla-kruopsciai-rengtas-tarptautinis-rusijos-teroro-aktas-120094314.
16. „Iniciatyvos pagal ES kibernetinio solidarumo aktą“. Lietuvos Respublikos krašto apsaugos ministerija. Žiūrėta 2026 m. balandžio 4 d. https://kam.lt/duk/es-kibernetinio-solidarumo-aktas/.
17. „Iš Lietuvos į Vokietiją ir JK savaime užsidegančias siuntas galėjo siųsti Rusija”. Verslo žinios. Žiūrėta 2026 m. balandžio 15 d. https://www.vz.lt/verslo-aplinka/2024/11/05/is-lietuvos-i-vokietija-ir-jk-savaime-uzsidegancias-siuntas-galejo-siusti-rusija.
18. „Išaiškinta ir sulaikyta asmenų grupė, organizavusi ir planavusi įvykdyti keturis teroro aktus, turinčius hibridinių tikslų“. Lietuvos Policija. Žiūrėta 2026 m. balandžio 15 d. https://policija.lrv.lt/lt/naujienos/isaiskinta-ir-sulaikyta-asmenu-gruoe-organizavusi-ir-planavusi-ivykdyti-keturis-teror-aktus-turincius-hibridiniu-tikslu-0hsd/.

19. „Išbandomi gaminiai, padėsiantys kovoti su kontrabandiniais balionais: ko galime tikėtis“. Lietuvos nacionalinis radijas ir televizija. Žiūrėta 2026 m. balandžio 8 d. https://www.lrt.lt/naujienos/lietuvoje/2/2843380/isbandomi-gaminiai-padesiantys-kovoti-su-kontrabandiniais-balionais-ko-galime-tiketis?srsltid=AfmBOoqxP8LmMAyjuJVLR-maKWwclj0ioSSXTr5KaY4di91PxYJFvc_S.
20. „Joint Declaration on EU-NATO Cooperation“. NATO. Žiūrėta 2026 m. vasario 20 d. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/01/10/joint-declaration-on-eu-nato-cooperation.
21. „Kaip vykdoma kibernetinė žvalgyba?“ Lietuvos Respublikos Valstybės saugumo departamentas. Žiūrėta 2026 m. balandžio 6 d. https://www.vsd.lt/verbavimas/kaip-vykdoma-kibernetine-zvalgyba.
22. „Launch of the EU-NATO Task Force“. Europos Komisija. Žiūrėta 2026 m. vasario 18 d. https://ec.europa.eu/commission/presscorner/detail/ga/statement_23_1705.
23. „Lietuvoje lankėsi NATO kovos su hibridinėmis grėsmėmis paramos komanda“. Lietuvos Respublikos užsienio reikalų ministerija. Žiūrėta 2026 m. vasario 20 d. https://www.urm.lt/naujienos/141/lietuvoje-lankesi-nato-kovos-su-hibridinemis-gresmemis-paramos-komanda:45568.
24. „Lietuvoje stiprinama pirmoji kibernetinės gynybos linija – steigiami 44 saugumo operacijų centrai“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 6 d. https://nksc.lrv.lt/lt/naujienos/lietuvoje-stiprinama-pirmoji-kibernetines-gynybos-linija-steigiami-44-saugumo-operaciju-centrai-1et/.
25. „Lietuvos dalyvavimas ES bendroje saugumo ir gynybos politikoje (BSGP)”. Lietuvos Respublikos užsienio reikalų ministerija. Žiūrėta 2026 m. vasario 11 d. https://www.urm.lt/lietuvos-saugumo-politika/lietuvos-dalyvavimas-es-bendroje-saugumo-ir-gynybos-politikoje-bsgp/309.
26. „Lietuvos kariuomenės Kibernetinės gynybos valdyba“. Lietuvos Respublikos krašto apsaugos ministerija,. Žiūrėta 2026 m. balandžio 4 d. https://kam.lt/duk/lietuvos-kariuomenes-kibernetines-gynybos-valdyba/.
27. „Lietuvos Respublikos Prezidento Gitano Nausėdos kalba strateginės politikos konferencijoje „Universitetai, formuojantys ateitį: atsparios visuomenės kūrimas per inovacijas ir visuotinį poveikį“. Lietuvos Respublikos Prezidentas. Žiūrėta 2025 m. lapkričio 15 d. https://lrp.lt/lt/lietuvos-respublikos-prezidento-gitano-nausedos-kalba-strategines-politikos-konferencijoje-universitetai-formuojantys-ateiti-atsparios-visuomenes-kurimas-per-inovacijas-ir-visuotini-poveiki/46153.

28. „Lietuvos, Latvijos ir Lenkijos Premjerai paskelbė bendrą deklaraciją dėl išorinių sienų apsaugos stiprinimo ir atsako į hibridines grėsmes“. Lietuvos Respublikos Vyriausybė. Žiūrėta 2026 m. vasario 27 d. https://lrv.lt/lt/naujienos/lietuvos-lenkijos-ir-latvijos-premjerai-paskelbe-bendra-deklaracija-del-isoriniu-sienu-apsaugos-stiprinimo-ir-atsako-i-hibridines-gresmes-7aaX/.
29. „LT72 – pasirengimo ekstremaliosioms situacijoms programėlė“. Lietuvos Respublikos Vidaus reikalų ministerija,. Žiūrėta 2026 m. balandžio 8 d. https://vrm.lrv.lt/lt/pasirengimo-ekstremaliosioms-situacijoms-programele-lt72/.
30. „Ministrų kabinetas pritarė atnaujintam Nacionalinės saugumo strategijos projektui“. Lietuvos Respublikos Vyriausybė. Žiūrėta 2026 m. vasario 25 d. https://lrv.lt/lt/naujienos/ministru-kabinetas-pritare-atnaujintam-nacionalines-saugumo-strategijos-projektui-myyf.
31. „Nacionalinis koordinavimo centras“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 4 d. https://www.nksc.lt/nkc/.
32. „Nacionalinis saugumas”. Lietuvos Respublikos krašto apsaugos ministerija. Žiūrėta 2026 m. vasario 26 d. https://kam.lt/duk/nacionalinio-saugumo-strategija/.
33. „NATO 2022 Strategic Concept“. NATO. Žiūrėta 2026 m. vasario 18 d. https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept.
34. „Naujame Lietuvoje kibernetinio saugumo registre – beveik 1500 organizacijų iš 18 sektorių”. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 24 d. https://nksc.lrv.lt/lt/naujienos/naujame-lietuvoje-kibernetinio-saugumo-registre-beveik-1500-organizaciju-is-18-sektoriu/.
35. „Nelaimių nelaukiama: valstybinė priešgaisrinė gelbėjimo tarnyba stiprina pasirengimą realioms grėsmėms“. Priešgaisrinės apsaugos ir gelbėjimo tarnybos departamentas prie vidaus reikalų ministerijos. Žiūrėta balandžio 8 d. https://pagd.lrv.lt/lt/naujienos/nelaimiu-nelaukiama-valstybine-priesgaisrine-gelbejimo-tarnyba-stiprina-pasirengima-realioms-gresmems-9Xr/.
36. „NKSC fiksavo du kibernetinius incidentus, susijusius su muzikos transliacijomis“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 4 d. https://www.nksc.lt/naujienos/nksc_fiksavo_du_kibernetinius_incidentus_susijusiu.html.
37. „NKVC atidžiai stebi situaciją dėl platinamų grasinančių pranešimų ugdymo įstaigoms ir teikia rekomendacijas“. Lietuvos Respublikos Vyriausybė. Žiūrėta 2026 m. balandžio

14 d. https://lrv.lt/lt/naujienos/nkvc-atidziai-stebi-situacija-del-platinamu-grasinanciu-pranesimu-ugdymo-istaigoms-ir-teikia-rekomendacijas/.

38. „Patogi ir interaktyvi mokymosi platforma“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 7 d. https://www.nksc.lt/mokymai/.
39. „Policijai gavus 850 grasinimų susprogdinti įstaigas, Požėla ragina nepanikuoti: tai yra koordinuota ataka“. Lietuvos nacionalinis radijas ir televizija. Žiūrėta 2026 m. balandžio 14 d. https://www.lrt.lt/naujienos/lietuvoje/2/2099522/policijai-gavus-850-grasinimu-susprogdinti-istaigas-pozela-ragina-nepanikuoti-tai-yra-koordinuota-ataka.
40. „Policijos ir prokuratūros smūgis „balionų“ konkrabandos organizatoriams“. Lietuvos Kriminalinės policijos biuras. Žiūrėta 2026 m. kovo 25 d. https://lkpb.policija.lrv.lt/lt/naujienos/policijos-ir-prokuraturos-smugis-balionu-konkrabandos-organizatoriams-wJa/.
41. „Prasidėjo nacionalinės pratybos „Kibernetinis skydas – TrustEx“: sveikatos ir vandentvarkos organizacijos mokosi sektorinės sąveikos“. Nacionalinis kibernetinio saugumo centras. Žiūrėta 2026 m. balandžio 7 d. https://www.nksc.lt/naujienos/prasidejo_nacionalines_pratybos_kiberneti_03d18fdf.html.
42. „Prevencinių reidų pasienio rajonuose rezultatai“. Lietuvos Policija. Žiūrėta 2026 m. kovo 25 d. https://policija.lrv.lt/lt/naujienos/reidu-pasienyje-rezultatai-kJ96/.
43. „Seimas pritarė siūlymams dėl bepiločių orlaivių ir kitų skraidančių objektų kontrolės stiprinimo“. Lietuvos Respublikos Seimas. Žiūrėta 2026 m. balandžio 15 d. https://www.lrs.lt/sip/portal.show?p_r=35435&p_t=290018&printVersion=1.
44. „Sukurtas įrankis, skaičiuojantis tikimybę, kad oro uostą pasieks kontrabandiniai balionai“. Lietuvos nacionalinis radijas ir televizija. Žiūrėta 2026 m. balandžio 8 d. https://www.lrt.lt/naujienos/mokslas-ir-it/11/2762172/sukurtas-irankis-skaiciuojantis-tikimybe-kad-oro-uosta-pasieks-kontrabandiniai-balionai?srsltid=AfmBOooU5pOhK_hwcstGoAgHo1nCEIRdJJNVj_STyQdqAqBEexd8itZr.
45. „Teisės aktų rūšys“. Europos Sąjunga. Žiūrėta gegužės 4 d. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_lt.
46. „The Council of Europe: key facts“. Council of Europe. Žiūrėta 2025 m. lapkričio 8 d. https://www.coe.int/en/web/portal/the-council-of-europe-key-facts.
47. „Vilniaus oro uostas atnaujino darbą, bet dienos metu gali vėluoti skrydžiai“. Lietuvos radijas ir televizija. Žiūrėta 2025 m. lapkričio 8 d.

https://www.lrt.lt/naujienos/verslas/4/2726153/vilniaus-oro-uostas-atnaujino-darba-bet-dienos-metu-gali-veluoti-skrydziai.

48. „Vilniaus rajone – taktinės pratybos „Sąveika 2023“ (foto)“. Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. Žiūrėta 2026 m. vasario 27 d. https://vsat.lrv.lt/lt/naujienos/vilniaus-rajone-taktines-pratybos-saveika-2023-foto/.
49. „Vyriausybė pritarė bepiločių orlaivių ir kitų skraidančių objektų kontrolės stiprinimui“. Lietuvos Respublikos Vyriausybė. Žiūrėta 2026 m. kovo 25 d. https://vrm.lrv.lt/lt/naujienos/vyriausybe-pritare-bepilociu-orlaiviu-ir-kitu-skraidanciu-objektu-kontroles-stiprinimui/.
50. „Vyriausybei JAV investuotojas perdavė technologiją kovai su kontrabandiniais balionais“. Lietuvos Respublikos Vyriausybė. Žiūrėta 2026 m. balandžio 8 d. https://lrv.lt/lt/naujienos/vyriausybei-jav-investuotojas-perdave-technologija-kovai-su-kontrabandiniais-balionais-ale8/.
51. „Visuomenės pasirengimas visuotinei gynybai“. Lietuvos Respublikos Krašto apsaugos ministerija. Žiūrėta 2026 m. vasario 25 d. https://kam.lt/visuomenes-pasirengimas-visuotinei-gynybai/.
52. „VSD: Rusijos GRU svetur naudojosi pažeidžiamais maršrutizatoriais vogti slaptą informaciją“. Lietuvos nacionalinis radijas ir televizija,. Žiūrėta balandžio 8 d. https://www.lrt.lt/naujienos/pasaulyje/6/2892299/vsd-rusijos-gru-svetur-naudojosi-pazeidziamais-marsrutizatoriais-vogti-slapta-informacija.
53. Council of the European Union. „Belarus: Council broadens scope of sanctions regime to cover hybrid activities against EU member states“. Žiūrėta 2026 m. kovo 2 d. https://www.consilium.europa.eu/en/press/press-releases/2025/12/15/belarus-council-broadens-scope-of-sanctions-regime-to-cover-hybrid-activities-against-eu-member-states/.
54. Europos Vadovų Taryba. *„Hibridinės grėsmės”.* Žiūrėta 2026 m. sausio 23 d. https://www.consilium.europa.eu/lt/policies/hybrid-threats/.
55. Lietuvių kalbos žodynas. „Hibridinis reikšmė”. Žiūrėta 2025 m. lapkričio 15 d. https://www.lietuviuzodynas.lt/terminai/Hibridinis.
56. Lisboa, Laura. „How to Protect the EU against Hybrid Threats“. *Policy Brief,* 2023 m. liepos 9 d. https://youngthinkers.ceps.eu/how-to-protect-the-eu-against-hybrid-threats/.

SANTRAUKA LIETUVIŲ KALBA

Šiandieninėje, ypatingai įtemptoje geopolitinėje situacijoje, hibridinės grėsmės yra vienas iš sudėtingiausių ir greičiausiai besikeičiančių reiškinių tiek Lietuvoje, tiek ir Europoje. Karas Ukrainoje, migrantų krizė, meteorologiniai balionai, dronai ir kitos hibridinio pobūdžio atakos tapo didžiuliu iššūkiu Lietuvos nacionaliniam saugumui. Hibridinės grėsmės atskleidė, jog vien tik stipri valstybės karinė galia, nebegarantuoja apsaugos nuo netradicinių ir daugialypių priemonių panaudojimo, siekiant paveikti gyventojų saugumo jausmą, pasitikėjimą valstybinėmis institucijomis ir valstybės stabilumą. Įvertinus tai, valstybės yra priverstos reaguoti į kasdien kylančius naujus iššūkius, keisti ir adaptuoti teisinį reglamentavimą, naudojamas apsaugos priemones, didinti gyventojų sąmoningumą ir stiprinti tarptautinį bendradarbiavimą. Baigiamojo darbo tema - „Hibridinės grėsmės kaip iššūkis Lietuvos nacionaliniam saugumui“. Tyrimo tikslas – išanalizuoti hibridines grėsmes (meteorologinių balionų incidentus ir kibernetinius išpuolius) kaip kompleksinį iššūkį Lietuvos nacionaliniam saugumui. Baigiamojo darbo tikslui įgyvendinti iškelti 5 uždaviniai: išanalizuoti hibridinių grėsmių sampratą ir raidą teoriniu aspektu, išanalizuoti nacionalinio saugumo sampratą hibridinių grėsmių kontekste, išnagrinėti Europos Sąjungos, NATO strategijas ir partnerystę, hibridinių grėsmių kontekste, išanalizuoti Lietuvos nacionalinio saugumo strategiją ir priemones, kovojant su hibridinėmis grėsmėmis, identifikuoti (pasirinktų hibridinių grėsmių) meteorologinių balionų ir kibernetinių išpuolių keliamus iššūkius Lietuvos nacionaliniam saugumui ir teisinio reglamentavimo pasikeitimus. Baigiamasis darbas sudarytas iš santrumpų sąrašo, įvado, trijų skyrių, išvadų, literatūros sąrašo, santraukų lietuvių, anglų kalbomis. Pirmajame baigiamojo darbo skyriuje pristatomas hibridinių grėsmių atsiradimas, pateikiamas jų apibrėžimas, rūšys, atskleidžiamas sąvokos daugialypiškumas, taip pat aptariama nacionalinio saugumo sąvoka, jos raida, teoriniai aspektai, pristatomi pagrindiniai saugumo sektoriai, „pilkoji zona”, analizuojama hibridinių grėsmių ir nacionalinio saugumo koreliacija. Antrajame skyriuje nagrinėjami tarptautiniai Europos Sąjungos, NATO komunikatai, dokumentai ir teisės aktai, strategijos kovojant su hibridinėmis grėsmėmis, atskleidžiamas organizacijų bendradarbiavimo būtinumas. Analizuojami Lietuvos nacionaliniai teisės aktai reglamentuojantys nacionalinį saugumą sąsajoje su hibridinėmis grėsmėmis. Trečiajame skyriuje, analizuojami meteorologinių balionų ir kibernetinių išpuolių atvejai, atskleidžiama jų, kaip hibridinių grėsmių įtaką Lietuvos nacionaliniam saugumui, pristatomi teisinio reguliavimo pokyčiai, naujų priemonių atsiradimas ir įgyvendinimas. Darbo pabaigoje pateikiamos išvados: 1) hibridinių grėsmių reiškinys sunkiai apibrėžiamas dėl nuolat vykstančių technologinių, geopolitinių ir kitų pasikeitimų, tačiau sutinkama, kad tai yra prievartinių ir ardomųjų veiklų, konvencinių ir nekonvencinių metodų derinys, naudojamas valstybinių ar nevalstybinių subjektų, siekiančių priešiškų tikslų, tačiau neskelbiant karo ir išliekant žemiau oficialaus karo ribos. Į šią sąvoką patenka karinių ir nekarinių

priemonių, tokių kaip diplomatinis, ekonominis spaudimas, kibernetiniai išpuoliai, dezinformacija panaudojimas. Identifikuoti kylančias grėsmės ir jų šaltinį ypač sudėtinga dėl subjektų veikimo „pilkojoje zonoje“, neaiškaus priešo buvimo ir oficialaus karo nepaskelbimo. 2) Nacionalinis šalies saugumas yra suprantamas, kaip valstybės teritorijos, suvereniteto ir jos gyventojų apsauga nuo išorinių ir vidinių grėsmių. Nacionaliniam saugumui įtaką daro aplinkosaugos, kariniui, ekonominiui, kibernetiniui, socialiniui ar politiniui valstybės sektoriui kylančios grėsmės. Pastarųjų metų įvykiai: „Ikea“ padegimas, savaime užsidegančios siuntos ir kt. parodė, kad Lietuva susiduria su Rusijos ir Baltarusijos vykdomais hibridiniais išpuoliais ir tai tiesiogiai veikia šalies nacionalinį saugumą. 3) Europos Sąjunga ir NATO vykdo kryptingą ir nuolatinį darbą hibridinių grėsmių prevencijos ir kovos srityje. ES parengti veiksmų planai, strategijos ir kiti dokumentai, rodo, jog hibridinių grėsmių keliami pavojai yra realūs ir toliau išlieka prioritetiniu Europos Sąjungos klausimu saugumo srityje. NATO užtikrina kolektyvinę gynybą, atgrasymą ir reagavimą, o Europos Sąjunga kuria teisėkūros, reguliavimo ir vidaus atsparumo stiprinimo priemones. 4) Įgyvendinant nacionalinio saugumo strategijos tikslus, valstybė imasi aktyvių priemonių kovojant su iškilusiomis hibridinėmis grėsmėmis: priimtas naujas Krizių valdymo ir civilinės saugos įstatymas, įkurtas Nacionalinis krizių valdymo centras, patvirtinta Civilinės saugos stiprinimo ir plėtros programa, gyventojai šviečiami hibridinių grėsmių ir pilietinio pasipriešinimo srityje, organizuojamos bendros valstybinių institucijų pratybos kritinės infrastruktūros apsaugos srityje. 5) Meteorologinių balionų naudojimas gabenant akcizais apmokestinamas prekes iš Baltarusijos į Lietuvą peržengė tradicinės kontrabandos ribas, įgijo hibridinių grėsmių pobūdį ir tapo tikru iššūkiu Lietuvos nacionaliniam saugumui. Lietuvos valstybės atsakas į šią grėsmę yra kompleksinis, apimantis tiek teisės aktų pakeitimus, tiek ir krizių valdymo, tarpinstitucinio bendradarbiavimo, bei kitų priemonių įgyvendinimo visumą. Atlikti pakeitimai rodo, jog teisinis reguliavimas nėra pakankamas. 6) Kibernetinės atakos vis dažniau naudojamos kaip netiesioginio poveikio priemonė, kuria siekiama sutrikdyti institucijų veiklą, paveikti visuomenę, skleisti dezinformaciją, mažinti pasitikėjimą valstybe ir kelti nesaugumo jausmą, neperžengiant atviro karinio konflikto ribų. Lietuvos atsakas į kibernetines grėsmes yra nuoseklus ir sisteminis. Tą rodo kibernetinio saugumo įstatymo atnaujinimas, kuriuo Lietuvos teisinėje sistemoje pradėta įgyvendinta ES direktyva TIS2, išplėstas kibernetinio saugumo subjektų ratas, sugriežtinta atsakomybė, piniginės baudos už kibernetinio saugumo pažeidimus. Taip pat visa apimtimi pradėtas taikyti ES Reglamentas 2019/881 (Kibernetinio saugumo aktas), ir ES Reglamentas 2021/887, kurio pagrindu Lietuvoje pradėjo veikti Nacionalinio koordinavimo centras, pradėta SOC/CSIRT sistemų plėtra ir kitos priemonės.

SANTRAUKA ANGLŲ KALBA

In today's particularly tense geopolitical situation, hybrid threats have become one of the most complex and rapidly evolving phenomena both in Lithuania and across Europe. The war in Ukraine, the migrant crisis, meteorological balloons, drones, and other hybrid-type attacks have become major challenges to Lithuania's national security. Hybrid threats have revealed that strong military power alone no longer guarantees protection against unconventional and multifaceted methods used to influence the population's sense of security, trust in state institutions, and the stability of the state. In response, states are forced to react to new daily challenges, adapt legal regulations, improve protection measures, increase public awareness, and strengthen international cooperation. The topic of this thesis is "Hybrid Threats as a Challenge to Lithuania's National Security." The aim of the research is to analyze hybrid threats (meteorological balloon incidents and cyberattacks) as a complex challenge to Lithuania's national security. To achieve this goal, five objectives were set: to analyze the concept and development of hybrid threats from a theoretical perspective; to examine the concept of national security in the context of hybrid threats; to review European Union and NATO strategies and partnerships in the context of hybrid threats; to analyze Lithuania's national security strategy and measures for combating hybrid threats; and to identify the challenges posed by selected hybrid threats (meteorological balloons and cyberattacks) to Lithuania's national security and the related changes in legal regulation. The thesis consists of a list of abbreviations, an introduction, three chapters, conclusions, a bibliography, and summaries in Lithuanian and English. The first chapter presents the emergence of hybrid threats, their definition, types, and the multidimensional nature of the concept. It also discusses the concept of national security, its development and theoretical aspects, introduces the main security sectors and the "grey zone," and analyzes the correlation between hybrid threats and national security. The second chapter examines international legal acts, communications, documents, and strategies of the European Union and NATO related to combating hybrid threats, highlighting the necessity of cooperation between these organizations. It also analyzes Lithuanian national legal acts regulating national security in connection with hybrid threats. The third chapter analyzes cases of meteorological balloons and cyberattacks, revealing their impact as hybrid threats on Lithuania's national security. It also presents changes in legal regulation, the emergence of new measures, and their implementation. The conclusions of the thesis are as follows: The phenomenon of hybrid threats is difficult to define due to constant technological, geopolitical, and other changes. However, it is generally understood as a combination of coercive and disruptive activities, conventional and unconventional methods, used by state or non-state actors pursuing hostile objectives without formally declaring war and remaining below the threshold of official warfare. This concept includes the use of both military and non-military means such as diplomatic

and economic pressure, cyberattacks, and disinformation. Identifying emerging threats and their source is particularly difficult because actors operate in the "grey zone," where the enemy is unclear and war is not officially declared. National security is understood as the protection of a state's territory, sovereignty, and population from external and internal threats. National security is affected by threats arising in environmental, military, economic, cyber, social, or political sectors. Recent events such as the "Ikea" arson attack, spontaneously igniting parcels, and similar incidents demonstrated that Lithuania faces hybrid attacks carried out by Russia and Belarus, which directly affect the country's national security. The European Union and NATO are carrying out targeted and continuous work in the field of prevention and response to hybrid threats. EU action plans, strategies, and other documents demonstrate that hybrid threats are real and remain a priority issue for the European Union in the field of security. NATO ensures collective defense, deterrence, and response, while the European Union develops legislative, regulatory, and internal resilience-building measures. In implementing the objectives of the national security strategy, the state is taking active measures to combat hybrid threats: adopting a new Crisis Management and Civil Protection Law, establishing the National Crisis Management Center, approving the Civil Protection Strengthening and Development Program, educating citizens about hybrid threats and civic resistance, and organizing joint exercises among state institutions in the field of critical infrastructure protection. The use of meteorological balloons to transport excise goods from Belarus to Lithuania has exceeded the boundaries of traditional smuggling, acquired the characteristics of hybrid threats, and become a real challenge to Lithuania's national security. Lithuania's response to this threat is comprehensive, including both amendments to legal acts and the implementation of crisis management, interinstitutional cooperation, and other measures. The changes made demonstrate that legal regulation alone is not sufficient. Cyberattacks are increasingly used as a tool of indirect influence aimed at disrupting institutional activities, influencing society, spreading disinformation, reducing trust in the state, and creating a sense of insecurity without crossing the threshold of open military conflict. Lithuania's response to cyber threats is consistent and systematic. This is demonstrated by the updated Cybersecurity Law, through which Lithuania began implementing the EU NIS2 Directive, expanded the range of cybersecurity entities, strengthened liability, and introduced financial penalties for cybersecurity violations. In addition, EU Regulation 2019/881 (Cybersecurity Act) and EU Regulation 2021/887 have been fully implemented, leading to the establishment of the National Coordination Center in Lithuania, the development of SOC/CSIRT systems, and other measures.