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

Biuletenio tematika ir tema
Tarptautiniai santykiai ir geopolitika

Biuletenio laidos antraštė, probleminis klausimas
Kova su Rusijos hibridiniais veiksmais Europoje

Esminiai žodžiai
hibridiniai veiksmai, kibernetinės atakos, NATO, ES, Ukraina

Serija ir registracijos numeris
ZD-2025-8

Leidimo data
2025-08-13

Leidimo vieta
Vilnius

Žanras
☒ Analitinė apžvalga ☐ Kita

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

Šaltiniai: nuo – iki
2015 05 19 – 2025 08 03

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

Citavimui (APA stiliumi)
Nacionalinė biblioteka, Informacijos analitikos skyrius (2025). *Kova su Rusijos hibridiniais veiksmais Europoje* (ZD-2025-8). Vilnius.

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

Turinio apžvalga
Apžvalgoje nagrinėjama:
- hibridinių grėsmių tipai;
- Rusijos hibridinės atakos (įskaitant kibernetines) prieš Ukrainą remiančias valstybes ir pačią Ukrainą;
- pasirengimas hibridinėms grėsmėms Lietuvoje;
- ES gynyba nuo hibridinių grėsmių.

1. Įžanga

Rusijos agresija prieš Ukrainą, prasidėjusi 2022 m. vasario 24 d., virto plataus masto konfliktu, kuriame fiziniu lygmeniu dalyvauja Ukrainos ir Rusijos reguliarios bei nereguliarios pajėgos (vadinamasis **kinetinis karas)**. Konfrontacija apima ir **hibridinius veiksmus –** šioje apžvalgoje taip apibūdinamas ribinis veikimas, vykdomas žemiau įprastinio karo slenksčio.

JAV karinėje doktrinoje tokio pobūdžio veiksmai vadinami „nereguliariu karu" „nereguliaria veikla" (angl. *irregular warfare, irregular activities*) , o Europoje dažniau įvardijami kaip „hibridinis karas" arba „hibridinės grėsmės". Vartojami ir tokie apibūdinamai kaip „pilkosios zonos veikla", „asimetrinis konfliktas", „netradicinis karas"[1].

[1] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*

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

Hibridinių veiksmų pavyzdžiai:

- informacijos ir įtakos skleidimas, įskaitant psichologines operacijas bei propagandą;
- puolamosios kibernetinės operacijos ir elektroninis karas;
- parama valstybiniams ir nevalstybiniams veikėjams, pavyzdžiui, diversantams ir statytiniams (angl. *proxy*);
- žvalgybos ir specialiųjų operacijų pajėgų veiksmai, įskaitant sabotažą ir diversiją;
- ekonominė prievarta[2].

Rusija, reaguodama į JAV ir Europos pagalbą Ukrainai, priėmė strateginį sprendimą eskaluoti hibridinį karą Europoje ir Amerikoje. Šiuo metu Rusija aktyviomis priemonėmis remia savo užsienio politikos tikslus:

- psichologinėmis operacijomis Europoje, JAV ir kitose šalyse daryti įtaką visuomenės nuomonei siekiant palenkti ją Rusijos naudai;
- priversti vyriausybes, įmones ar asmenis riboti ar nutraukti karinę ir kitokią pagalbą Ukrainai;
- atgrasyti Rusijos kariškius, vyriausybės pareigūnus ir piliečius nuo perbėgimo į Vakarus;
- skatinti nesutarimus tarp valstybių, ypač tarp NATO narių;
- griauti demokratines normas ir vertybes, kuriomis grindžiamos Vakarų politinės sistemos[3].

Daugelis taikinių yra vienaip ar kitaip susiję su Ukraina: nuo Ispanijoje nužudyto Rusijos karinio perbėgėlio[4] iki sabotažo aktų prieš bendroves, tokias kaip *Rheinmetall, Diehl Group* (Vokietija), *BAE Systems* (Jungtinė Karalystė, JK), EMCO (Bulgarija), kurios gamina ginklus Ukrainai[5]. Šalyse, kurios nesuteikė pagalbos Ukrainai (pvz. Vengrija, Serbija), nebuvo užfiksuota panašių incidentų (bent jau iki 2025 m. liepos)[6].

Jungtinės Karalystės (JK) lyderystė remiant Ukrainą didina grėsmę valstybei, teigiama JK vidaus kontržvalgybos ir saugumo agentūros MI5 generalinio direktoriaus Keno McCallumo pranešime (2024 m.)[7]. Pasak MI5 vadovo, Rusija siekia sukelti ilgalaikį chaosą Britanijoje ir Europoje, griebdamasi kibernetinių atakų, sabotažo, padegimų ir kitų ard0mųjų veiksmų. Norvegijos žvalgyba padarė išvadą, kad vienas iš pagrindinių Rusijos taikinių šalyje yra subjektai, susiję su ginklų tiekimu ir Ukrainos personalo mokymu[8].

Lietuva patyrė keletą atakų, kurių organizatorių reikia ieškoti Rusijoje: padegimų, sabotažo bandymų. Jos **detaliau nušviestos antrame apžvalgos skyriuje** kitų hibridinių Rusijos veiksmų kontekste.

---

[2] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[3] Ten pat.
[4] Gozzi, L. (2024 m. vasario 20 d.). Russian pilot Maxim Kuzminov who defected to Ukraine 'shot dead' in Spain. Prieiga per internetą: *https://www.bbc.com/news/world-europe-68337794*
[5] Wannenmacher, T. (2025 m. kovo 21 d.). Putin's shadow army in Europe: the invisible front. Prieiga per internetą: *https://www.mimikama.org/en/putin-39-s-shadow-army-in-europe-fact-check/*
[6] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[7] Barkhush, A. (2025 m. birželio 27 d.). MI5 Chief Warns of Russia's Intelligence Plotting "Mayhem" on UK and European Streets. Prieiga per internetą: *https://united24media.com/latest-news/mi5-chief-warns-of-russias-intelligence-plotting-mayhem-on-uk-and-european-streets-2915*
[8] Brandvold, S. (2024 m. lapkričio 8 d.). Norwegian Intelligence Assessment on Russian Interference: *https://jamestown.org/program/norwegian-intelligence-assessment-on-russian-interference/*

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

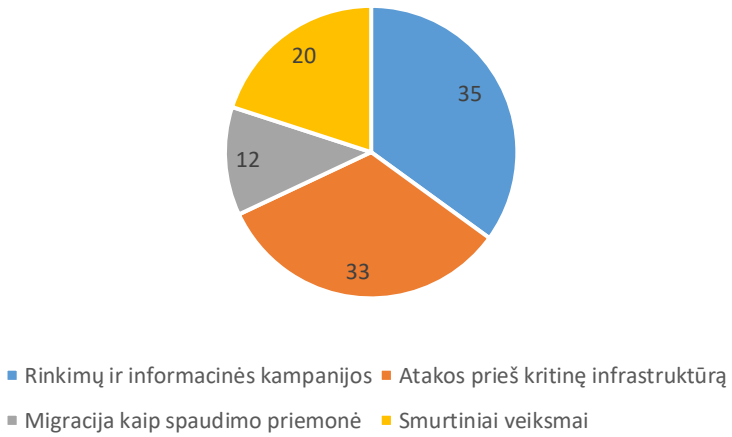
Greta to, apžvalgoje referuojama apie:

- Europoje vykdytas Rusijos kibernetines atakas (3 skyrius),
- hibridinių grėsmių suvokimą Lietuvoje (4 skyrius),
- ES ir NATO priemones hibridiniams veiksmams atremti (5 skyrius).

2. Rusijos hibridinis karas Europoje

Rusijos hibridiniai veiksmai fiksuojami keliose viešai prieinamose duomenų bazėse, kurias rengia, pvz., Leideno universitetas (Nyderlandai)[9,10] , JAV komisija Europos saugumui ir bendradarbiavimui (JAV Helsinkio komisija)[11].

1 grafikas. Hibridinės operacijos visame pasaulyje, kurias organizavo Rusija (arba sukėlė tokių įtarimų) nuo 2022 m. vasario iki 2024 m. lapkričio, proc.
Operacijų skaičius – 150
© (duomenys) JAV Helsinkio komisija (U.S. Helsinki Commission)[12] © (grafika) Lietuvos nacionalinė biblioteka



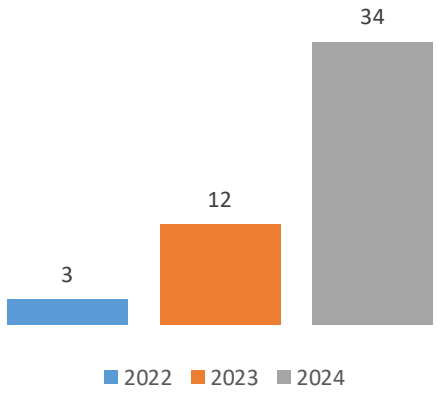
Detaliau apžvelgsime Rusijos veiksmus, įtrauktus į **Strateginių ir tarptautinių tyrimų centro** duomenų bazę (angl. *Center for Strategic and International Studies*, CSIS)[13], kurioje pateikiami **Rusijos ardomieji veiksmai Europoje** nuo 2022 m. Duomenys apima Rusijos išpuolius ir sąmokslus, kurie padarė (arba siekė padaryti) materialų fizinį poveikį. Kitaip nei JAV Helsinkio komisijos bazėje (žr. 1 grafiką aukščiau), į CSIS bazę neįtrauktos kibernetinės atakos, dezinformacijos kampanijos ir bandymai paveikti

[99] Dobbinga, B. (n. d.). Research: Europe increasingly targeted by Russian sabotage. Prieiga per internetą: *https://www.universiteitleiden.nl/en/news/2025/01/research-europe-increasingly-targeted-by-russian-sabotage*
[10] Schuurman, B. (n. d.) Russian Operations Against Europe Dataset. Prieiga per internetą: *https://doi.org/10.7910/DVN/TQ0FMQ*
[11] Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory. A Report by the U.S. Helsinki Commission Staff. (2024 m. gruodžio 12 d.). Prieiga per internetą: *https://www.csce.gov/publications/spotlight-on-the-shadow-war-inside-russias-attacks-on-nato-territory/*
[12] U.S. Helsinki Commission. (2024 m. gruodžio 16 d.). Identified Hybrid Operations. Prieiga per internetą: *https://x.com/HelsinkiComm*
[13] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*

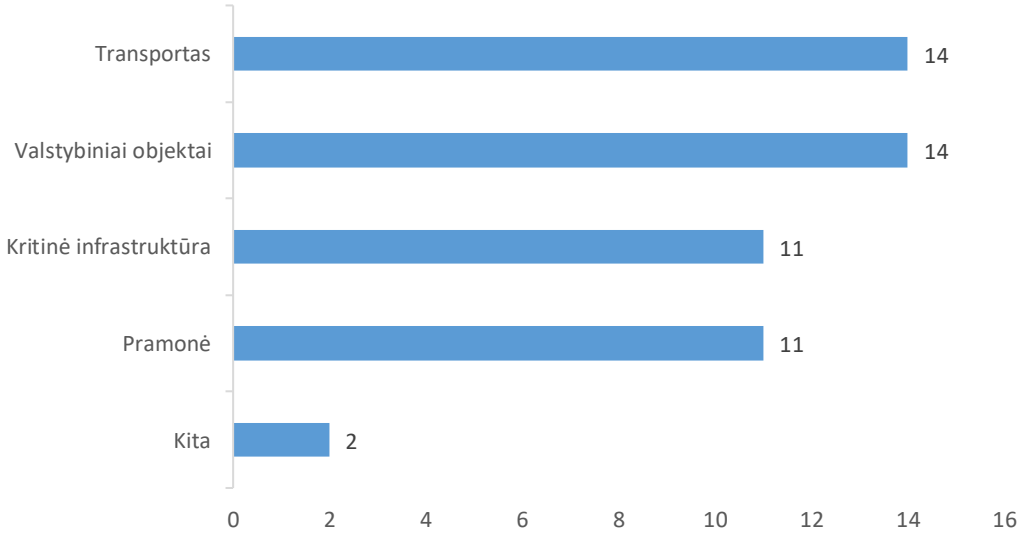
demokratinius procesus Vakarų valstybėse, bet **įtraukti incidentai, kai Rusijos kibernetinės ar elektroninės atakos padarė pastebimą materialinę žalą**.

Rusijos agentai puolė įvairius taikinius – nuo kritinės infrastruktūros iki transporto objektų. Naudoti įvairūs ginklai ir taktika – nuo sprogmenų iki fizinių įrankių, tokių kaip laivų inkarai.

2 grafikas. CSIS fiksuotų išpuolių dinamika 2022-2024 m., incidentų skaičius
Viso 49 atvejai
© (duomenys) CSIS[14] © (grafika) Lietuvos nacionalinė biblioteka



3 grafikas. Rusijos išpuolių Europoje taikiniai 2022 m. – 2025 m. kovą, incidentų skaičius*
Viso 52 atvejai
© (duomenys) CSIS[15] © (grafika) Lietuvos nacionalinė biblioteka



[14] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[15] Ten pat.

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

*) 2 grafike nurodyti 49 incidentai, o 3 grafike – 52, kadangi pastarojo grafiko duomenys apima ir pirmus tris 2025 m. mėnesius. Kitas analitinis centras, Tarptautinis strateginių tyrimų institutas (*The International Institute for Strategic Studies*, IISS) per 2025 m. sausį-gegužę suskaičiavo 11 Rusijos išpuolių[16].

Rusijos taikiniai Europoje dažnai buvo susiję su transporto sektoriumi – trikdytas traukinių ir lėktuvų eismas. Kėsintasi ir į valstybinius taikinius, pvz., karines bazes bei pasienio punktus. Rusija taip pat vykdė išpuolius prieš ypatingos svarbos infrastruktūrą, pvz., vamzdynus ir povandeninius šviesolaidinius kabelius bei pramonę, daugiausiai gynybos įmones[17].

Jūrų, sausumos ir oro transporto objektai buvo pagrindiniai Rusijos aktyvių priemonių taikiniai. Pvz., 2022 m. Vokietijoje buvo pjaustomi geležinkelio kabeliai[18]. Rusija surengė keletą išpuolių prieš Lenkijos geležinkelių sistemą 2023 m. (diversantai radijo signalais įjungdavo traukinių avarinį stabdymą)[19]. Rusija taip pat taikėsi į lėktuvus, vykdydama elektronines atakas (GPS signalų trukdymas)[20].

Rusija gadino ypatingos svarbos infrastruktūros objektus, įskaitant povandeninius kabelius ir vamzdynus (ši tema anksčiau nagrinėta apžvalgoje ZD-2025-3). Privatus sektorius, ypač gynybos pramonės įmonės, buvo dažni Rusijos atakų taikiniai.

Dvi didžiausios Europos karinės pagalbos Ukrainai teikėjos – Vokietija ir JK – patyrė išpuolius prieš gynybos gamyklas. Pvz., 2024 m. gegužę Berlyne esančioje *Diehl Group* gamykloje, kurioje gaminamos Ukrainoje naudojamos *IRIS-T* žemė-oras raketos, kilo didelis gaisras[21]. Mėnesiu anksčiau įvyko sprogimas Pietų Velso gamykloje, priklausančioje didžiausiai JK ginklų gamintojai *BAE Systems*, tiekusiai Ukrainai šaudmenis, ginklus ir kitokią gynybos įrangą[22].

Trys Rusijos ir Vokietijos piliečiai planavo sprogdinimus bei padegimus JAV karinėse bazėse Vokietijoje, kurios buvo susijusios su Ukraina[23]. JAV bazėje Grafenvere, Vokietijoje, Ukrainos kariai buvo mokomi valdyti *M1 Abrams* tankus[24].

Ispanijoje esančiame sandėlyje, kuriame buvo laikoma Ukrainai skirta ryšių įranga, įvyko sprogimas. Sprogdinti ir Bulgarijos ginklų gamintojos ir prekybininkės EMCO šaudmenų sandėliai. Tai įvyko praėjus vos kelioms dienoms po to, kai Bulgarija paskelbė oficialiai prisijungsianti prie koalicijos, tiekiančios šaudmenis Ukrainai[25].

2025 m. sausio mėn. Švedijoje sugadinus kabelį, esantį prie kelio E22, trumpam buvo išvesta iš rikiuotės 30 telekomunikacijos bokštų[26].

Dažniausiai Rusijos šešėliniame kare naudojami ginklai buvo sprogmenys arba padegamosios medžiagos, įskaitant bombas.

---

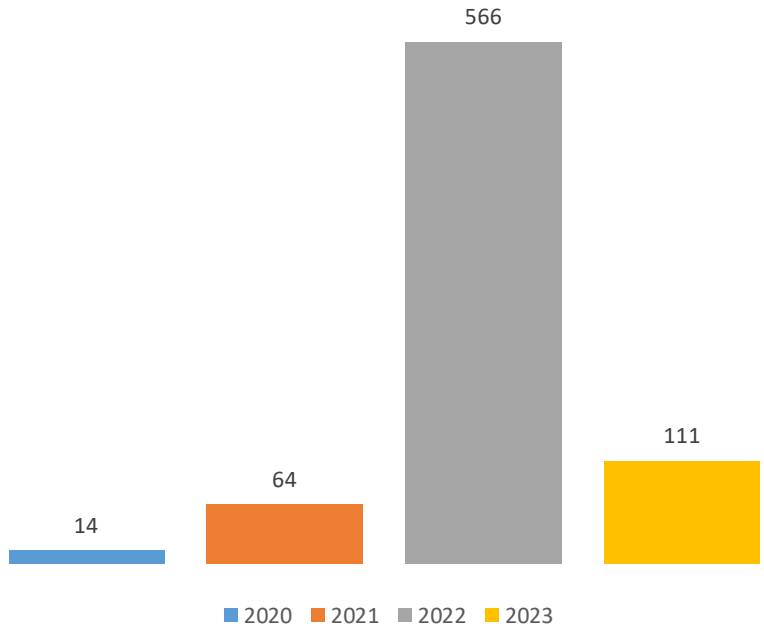
[16] US, Europe see Putin reining in Russia's unruly hybrid war. (2025 m. rugpjūčio 2 d.) Prieiga per internetą: *https://www.bloomberg.com/news/articles/2025-08-02/us-and-europe-see-putin-reining-in-russia-s-unruly-hybrid-war*
[17] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[18] Repeat sabotage suspected after German railway cables cut. (2022 m. gruodžio 17 d.). Prieiga per internetą: *https://www.euronews.com/2022/12/17/germany-rail-sabotage*
[19] Kość, W. (2023 m. rugpjūčio 28 d.). Polish train chaos blamed on radio hackers. Prieiga per internetą: *https://www.politico.eu/article/poland-train-chaos-radio-hackers-russia-ukraine-war/*
[20] International aviation community pressures Russia: GNSS signal interference must stop. (2025 m. liepos 8 d.). Prieiga per internetą: *https://www.madeinvilnius.lt/en/transport/airport/The-international-aviation-community-is-pressuring-Russia-to-stop-jamming-GNSS-signals./*
[21] Germany: Fire breaks out at Berlin metal factory. (2024 m. balandžio 5 d.). Prieiga per internetą: *https://www.dw.com/en/germany-fire-breaks-out-at-berlin-metal-factory/a-68992842*
[22] Suspected Russian sabotage: The great return of Kremlin agents to Europe? (2024 m. gegužės 10 d.). Prieiga per internetą: *https://www.france24.com/en/europe/20240510-suspected-russian-sabotage-campaigns-great-return-russian-agents-europe*
[23] Mekhennet, S. et al. (2024 m. liepos 10 d.). Russia recruits sympathizers online for sabotage in Europe, officials say. Prieiga per internetą: *https://www.washingtonpost.com/world/2024/07/10/russia-sabotage-europe-ukraine/*
[24] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[25] Ten pat.
[26] King, J., Feng, J. (2025 m. birželio 30 d.). Multiple Cell Towers Sabotaged Across NATO Nation: What To Know. Prieiga per internetą: *https://www.newsweek.com/nato-telecommunications-sweden-cell-towers-sabotage-2092514*

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

Rusijos agentai panaudojo elektrinius masažuoklius su magnio pagrindu pagaminta degia medžiaga. Jie buvo **išsiųsti iš Lietuvos** ir sprogo DHL logistikos centruose Leipcige (Vokietija), Birmingeme (Anglija) ir Jablonove (Lenkija)[27,28]. Lenkijos prokuratūra spėja, kad Rusijos tikslas buvo išbandyti tokių siuntinių, kurie galiausiai turėjo būti išsiųsti į JAV ir Kanadą, perdavimo kanalą. Vokietijos policija, išbandžiusi padegamųjų įtaisų modelius, pažymėjo, kad užsidegus magniui, daugumos lėktuvų gaisrų gesinimo sistemoms jį būtų sunku užgesinti[29].

Reaguodamos į Rusijos agresiją prieš Ukrainą, Europos šalys išsiuntė nemažai Rusijos diplomatų.

4 grafikas. Išsiųstų Rusijos diplomatų skaičius, 2020-2023 m. (visos pasaulio šalys)
© (duomenys) Statista[30] © (grafika) Lietuvos nacionalinė biblioteka



Praradus patyrusių kadrų diplomatinėse atstovybėse, sumažėjo Rusijos operacijų profesionalumas, nes imta pasikliauti atsitiktiniais agentais (vaizdžiai kalbant, „iš gatvės“) ir nusikaltėliais. MI5 generalinio direktoriaus K. McCallumo pranešime (2024 m.) teigiama, kad Rusijos agentai su vis didesniu neapdairumu vykdė padegimus, sabotažą ir kitokius ardomuosius veiksmus[31].

Rusijos agentų „profesionalumo“ lygį iliustruoja **keli incidentai Lietuvoje**.

Nepilnametis Ukrainos pilietis Vilniaus IKEA parduotuvės patalynės skyriuje 2024 m. gegužės 8 d. padėjo padegamąjį įtaisą, kuris kitą dieną sprogo. Nusikaltėlis buvo sulaikytas pakeliui į Latviją, kur jis galimai turėjo įvykdyti kitą išpuolį. Paauglys buvo užverbuotas internetu pogrindiniame Rusijos tinkle, kuriam vadovavo Rusijos specialiosios tarnybos. Nurodymai nusikaltėliui ir kitiems užverbuotiems asmenims buvo siunčiami per „Telegram“

[27] Incendiary parcels sent from Lithuania as part of Russian covert operation. (2024 m. lapkričio 5 d.). Prieiga per internetą: *https://www.lrt.lt/en/news-in-english/19/2405496/incendiary-parcels-sent-from-lithuania-as-part-of-russian-covert-operation-media*
[28] Žiniasklaida: iš Lietuvos siųstos savaime užsidegančios siuntos buvo dalis slaptos Rusijos operacijos. (2024 m. lapkričio 5 d.). Prieiga per internetą: *https://www.15min.lt/naujiena/aktualu/lietuva/ziniasklaida-is-lietuvos-siustos-savaime-uzsidegancios-siuntos-buvo-dalis-slaptos-rusijos-operacijos-56-2336626*
[29] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[30] Number of Russian diplomats expelled from countries worldwide from 2010 to 2023. (2024 m. rugsėjo 30 d.). Prieiga per internetą: *https://www.statista.com/statistics/1267664/number-of-expelled-russian-diplomats/*
[31] Barkhush, A. (2025 m. birželio 27 d.). MI5 Chief Warns of Russia's Intelligence Plotting "Mayhem" on UK and European Streets. Prieiga per internetą: *https://united24media.com/latest-news/mi5-chief-warns-of-russias-intelligence-plotting-mayhem-on-uk-and-european-streets-2915*

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

kanalą, taip pat per Kinijos žinučių siuntimo programėlę „Zangi“[32]. Lietuvoje teisiamas jaunuolis savo kaltę pripažino[33].

Kolumbijos policija 2025 m. liepos mėn. pranešė sulaikiusi Lietuvoje ieškomą vyrą, kuris įtariamas bandymu įvykdyti išpuolį Šiauliuose prieš kompaniją, tiekiančią dronus Ukrainai. Sulaikytas Kolumbijos pilietis į Šiaulius iš Rusijos atvyko 2024 m. rugsėjo 2 dieną žvalgybiniais tikslais. Kitą dieną jis išvyko į Norvegiją. Jo tikslas buvo parengti teroro aktą ir taip sunaikinti arba bent jau apgadinti įmonės turtą[34].

Du ispanai 2024 m. rugsėjo mėn. Šiauliuose planavo padegti Ukrainą remiančią įmonę. Įtariama, kad ispanus išpuoliui pasamdė Rusijos žvalgyba. Ispanai įmonės nepadegė, o juos pasamdžiusius rusus bandė apgauti: siuntė jiems vaizdus, neva gaisras sukeltas. Nusikaltėliai buvo sulaikyti Rygoje. Pasak Lietuvos pareigūnų, **panašių Rusijos organizuotų atakų Lietuvoje buvo daugiau, tik ne visos dar paviešintos**[35]

Šešiems asmenims, tarp jų dviem Lietuvos piliečiams, Ugniui Ašmenai ir Dmitrijui Paulauskui, 2024 m. spalį pateikti kaltinimai dėl gaisro, kurį Rusijos „Wagner“ grupės[36] užsakymu įtariamieji sukėlė JK 2024 m. pavasarį.

Gaisras rytų Londone sukeltas dviejuose objektuose, įskaitant įmonę, vežusią siuntas į Ukrainą ir sandėliavusią *Starlink* palydovinę įrangą, kuri buvo skirta Ukrainai. Gaisrui užgesinti prireikė 60 ugniagesių. 2025 m. liepą U. Ašmena ir dar du asmenys pripažinti kaltais dėl padegimo, D. Paulauskas išteisintas dėl informacijos apie rengiamą išpuolį neatskleidimo[37, 38].

Europoje su Rusija siejami keli išpuoliai prieš asmenis.

Pvz., 2024 m. vasario mėn. Ispanijoje buvo nužudytas Rusijos sraigtasparnio pilotas Maksimas Kuzminovas, 2023 m. rugpjūtį pabėgęs iš Rusijos[39]. 2024 m. Lietuvoje įvykdytas išpuolis prieš Rusijos pilietį ir buvusį artimą nužudyto opozicijos lyderio Aleksejaus Navalno padėjėją Leonidą Volkovą. Užpuolikai sulaužė L. Volkovui ranką, bet jo neužmušė[40]. Estijoje vandalai nusitaikė į vidaus reikalų ministro Lauri Läänemetso automobilį[41].

Būta nesėkmingų sąmokslų nužudyti:

- Ukrainos prezidentą Volodymyrą Zelenskį (Lenkija, 2024 m. balandis)[42];
- tiriamosios žurnalistikos grupės „Bellingcat“ vadovą bulgarą Christą Grozevą (Austrija, 2023 m. vasaris)[43];

[32] IKEA padegimas Vilniuje: ukrainietis sprogmenis ir mobiliuosius slėpė geležinkelio stotyje. (2025 m. balandžio 10 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/2533737/ikea-padegimas-vilniuje-ukrainietis-sprogmenis-ir-mobiliuosius-slepe-gelezinkelio-stotyje*
[33] Pankūnas, G. (2025 m. gegužės 9 d.). „Ikea“ padegimo byla: terorizmu kaltinamas jaunuolis pripažįsta kaltę ir gailisi. Prieiga per internetą: *https://www.delfi.lt/news/daily/lithuania/ikea-padegimo-byla-terorizmu-kaltinamas-jaunuolis-pripazista-kalte-ir-gailisi-120108191*
[34] Gerdžiūnas, B. (2025 m. liepos 9 d.). Kolumbija sulaikė Lietuvos ieškomą vyrą: atvykęs iš Rusijos planavo išpuolį Šiauliuose. Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/2605258/kolumbija-sulaike-lietuvos-ieskoma-vyra-atvykes-is-rusijos-planavo-ispuoli-siauliuose*
[35] Salyga, G. (2022 m. lapkričio 20 d.). Naujos detalės apie planuotą teroro išpuolį Šiauliuose: ispanai bandė rusus apgauti. Prieiga per internetą: *https://www.delfi.lt/news/daily/lithuania/naujos-detales-apie-planuota-teroro-ispuoli-siauliuose-ispanai-bande-rusus-apgauti-120066046*
[36] LRT trumpai. Kas yra „Wagner“ grupuotė ir jos vadas Prigožinas?. (2023 m. birželio 24 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/2020610/lrt-trumpai-kas-yra-wagner-grupuote-ir-jos-vadas-prigozinas*
[37] Byloje dėl padegimo Londone – kaltinimai ir lietuviams: dirbo pagal „Wagner“ užsakymą. (2024 m. spalio 4 d.). Prieiga per internetą: *https://kauno.diena.lt/naujienos/pasaulis/konfliktai-nelaimes/byloje-del-padegimo-londone-kaltinimai-ir-lietuviams-dirbo-pagal-wagner-uzsakyma-1194516*
[38] 3 vyrai pripažinti kaltais padegę Londone su Ukraina susijusias įmones, tarp jų – lietuvis. (2025 m. liepos 8 d.). Prieiga per internetą: *https://www.lrt.lt/lituanica/aktualijos/751/2604910/3-vyrai-pripazinti-kaltais-padege-londone-su-ukraina-susijusias-imones-tarp-ju-lietuvis*
[39] Chiappa, C. et al. (2024 m. lapkričio 18 d.). The death of a Russian defector: Who failed Maxim Kuzminov? Prieiga per internetą: *https://www.politico.eu/article/maxim-kuzminov-russia-ukraine-defector-murder-fsb-spain-helicopter/*
[40] Žiniasklaida: lenkų prokurorai padarė išvadą, kad Nevzlinas „įkvėpė“ išpuolį prieš Volkovą. (2025 m. liepos 14 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/pasaulyje/6/2607056/ziniasklaida-lenku-prokurorai-padare-isvada-kad-nevzlinas-ikvepe-ispuoli-pries-volkova*
[41] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[42] Croucher, S. (2024 m. birželio 23 d.). Zelensky Assassination Plot Foiled: What to Know. Prieiga per internetą: *https://www.newsweek.com/zelensky-assassination-plot-foiled-what-know-2089353*
[43] Walker, S. (2025 m. kovo 10 d.). 'They came across as muppets': Christo Grozev on being target of Bulgarian spy ring. Prieiga per internetą: https://www.theguardian.com/world/2025/mar/10/they-came-across-as-muppets-christo-grozev-on-being-target-of-bulgarian-spy-ring

– Arminą Pappergerį, Vokietijos artilerijos ir tankų gamintojos „Rheinmetal", siunčiančios šaudmenis į Ukrainą, generalinį direktorių (apie tai pranešta 2024 m. gruodžio mėn.)[44,45]

Rusija ir Baltarusija pavertė nelegalius imigrantus ginklais prieš kelias pasienio šalis, tokias kaip Suomija, Latvija, Lietuva, Norvegija ir Lenkija[46]. Šios pasienio krizės, tikėtina, buvo surežisuotos siekiant daryti spaudimą valstybės institucijoms, eikvoti atakuojamų valstybių išteklius ir kurstyti kraštutinių dešiniųjų partijų retoriką, nukreiptą prieš imigrantus[47].

Apibendrinant duomenis galima skaičiuoti, kad Rusijos išpuolių kiekis Europoje nuo 2022 m. (3 išpuoliai) iki 2024 m. (34 išpuoliai) išaugo daugiau nei 10 kartų[48]. CSIS ekspertų vertinimu, nors Rusija naudoja gyvybei ir turtui pavojingas priemones, veiksmų mastas kol kas verčia manyti, kad Maskva labiau siekia atgrasyti nuo ginklų siuntimo ir kitokios pagalbos Ukrainai, o ne padaryti reikšmingą žalą. Iki šiol per išpuolius nukentėjo santykinai nedaug žmonių ir tai rodo, kad Rusija veikia su mažomis sąnaudomis ir tikimybe paneigti savo dalyvavimą. Vis dar žemas smurto lygis leidžia Maskvai prireikus eskaluoti teroristinius veiksmus iki didesnio masto kampanijos[49].

3. Rusijos kibernetinės atakos

Rusijos grėsmė įvertinta tiek ekspertiniu (minėti CSIS, IISS pranešimai), tiek NATO šalių žvalgybų lygmeniu. CSIS sudarė atskirą bazę, kurioje fiksuoti kibernetiniai incidentai nuo 2006 iki 2025 m. (bazė apima ne vien Rusijos veikimą)[50]. Su Rusija siejama šimtai kibernetinių atakų prieš taikinius Europoje, JAV ir kituose regionuose, kai bandyta rinkti žvalgybos duomenis, gadinti interneto svetaines, trikdyti paslaugų teikimą[51,52].

2016 m. žiemą ukrainiečiai patyrė elektros tinklų sutrikimą, kurį sukėlė kenkėjiška kompiuterio programa *Industoyer One*. Penktadalis Kijevo gyventojų kurį laiką neturėjo elektros. 2022 m. Rusijos ir Ukrainos karo pradžioje buvo surengta dar viena ataka (programa *Industoyer Two*), kuria buvo bandoma suderinti karines atakas iš oro ir kibernetines atakas, taikantis labai pakenkti Ukrainos elektros tiekimui[53].

2024 m. rugsėjo mėn. Vokietijos federalinė Konstitucijos apsaugos tarnyba (vok. *Bundesamt für Verfassungsschutz*, BfV) perspėjo apie padažnėjusius kibernetinius išpuolius, kuriuos vykdo Rusijos

[44] Körömi, C. (2025 m. sausio 28 d.). NATO: There was officially a Russian plot to kill European weapons chief. Prieiga per internetą: *https://www.politico.eu/article/nato-official-confirms-russian-plot-kill-european-weapons-chief-armin-papperger/*
[45] Germany decries Russian plot to assassinate Rheinmetall boss. (2024 m. gruodžio 7 d.). Prieiga per internetą: *https://www.dw.com/en/germany-decries-russian-plot-to-assassinate-rheinmetall-boss/a-69641234*
[46] Scutaru, G. (2024 m. rugsėjo 17 d.). Weaponization of Migration: A Powerful Instrument in Russia's Hybrid Toolbox. Prieiga per internetą: *https://www.hoover.org/research/weaponization-migration-powerful-instrument-russias-hybrid-toolbox*
[47] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[48] Ten pat.
[49] Jones, S. (2025 m. kovo 18 d.). Russia's Shadow War Against the West. Prieiga per internetą: *https://www.csis.org/analysis/russias-shadow-war-against-west*
[50] Significant Cyber Incidents. (n. d.). Prieiga per internetą: *https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents*
[51] Ten pat.
[52] Stuxnet. (2010 m.). Prieiga per internetą: *https://www.cfr.org/cyber-operations/stuxnet*
[53] Cerf, E. (2024 m. gegužės 17 d.). Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world. Prieiga per internetą: *https://news.ucsc.edu/2024/05/ukraine-cybersecurity/*

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

karinės žvalgybos (rus. santrumpa GRU, *ГРУ*) padalinys, žymimas numeriu 29155[54]. Ši grupuotė įtariama šnipinėjimu, sabotažu ir informacinėmis diversijomis prieš NATO ir ES šalis, taip pat tarptautines organizacijas[55]. BfV teigimu, padalinio kibernetinės operacijos nukreiptos į pagalbos teikimo Ukrainai trikdymą, taip pat taikomasi į infrastruktūrą[56]. Padalinys naudojo kenkėjiškas programas atakoms prieš Ukrainos organizacijas 2022 m. sausio mėn. (mėnesį prieš Rusijos invaziją į Ukrainą). Įtariama, kad grupuotė organizavo kibernetines atakas prieš Vokietijos socialdemokratų partiją ir kelias informacinių technologijų, logistikos ir aviacijos bei kosmoso sektorių įmones[57].

Lietuvos policija pranešė, kad 2025 m. liepos 14–17 d. teisėsaugos institucijos iš Vokietijos, Čekijos, Prancūzijos, Suomijos, Italijos, Lietuvos, Lenkijos, Ispanijos, Švedijos, Šveicarijos, Nyderlandų ir JAV vienu metu vykdė operaciją *Eastwood* prieš prorusišką programišių grupuotę *NoName057(16)*, kuri kenkė kibernetinėmis *DDoS* tipo atakomis[58]. Tokios atakos metu interneto svetainė tyčia užtvindoma didžiuliu duomenų srautu, kad taptų nepasiekiama vartotojams[59].

Su *NoName057(16)* grupuote siejami asmenys iš pradžių taikėsi į Ukrainą, o vėliau dėmesį nukreipė į šalis, remiančias ja kare su Rusija. Viena iš atakų buvo surengta per NATO viršūnių susitikimą Nyderlanduose. 2023 ir 2024 metais grupuotė dalyvavo atakose prieš Švedijos institucijas bei bankų interneto svetaines. Nuo tyrimų pradžios 2023 m. lapkritį, Vokietijoje užfiksuota 13 atakų bangų, nukreiptų prieš maždaug 230 įmonių ir institucijų. 2023 m. ir 2024 m. birželį kibernetinės atakos buvo surengtos Šveicarijoje per svarbius Ukrainai renginius. Šios atakos buvo sėkmingai suvaldytos, išvengiant reikšmingų veiklos sutrikimų[60].

NoName057(16) – tai ideologinė hakerių (programišių) grupuotė, atvirai reiškianti paramą Rusijai.

Grupei, turinčiai daugiau nei 4 tūkst. jos veiklą palaikančių asmenų, pavyko sukurti ir nuosavą *botnet* tinklą – šimtus serverių sudarančią infrastruktūrą, naudotą atakų pajėgumui didinti. Skleisdama raginimus veikti, dalindamasi instrukcijomis bei programų atnaujinimais ir verbuodama savanorius, grupuotė naudojosi prorusiškais kanalais, interneto forumais, nišinėmis pokalbių grupėmis socialiniuose tinkluose bei žinučių siuntimo programėlėse. Savanoriai dažnai kviesdavo prisijungti pažįstamus iš žaidimų ar hakerių (programišių) bendruomenių, taip formuodami nedideles verbavimo grupes. Jie naudojo platformas, kurios supaprastindavo techninius procesus ir pateikdavo aiškias instrukcijas, leidžiančias naujokams greitai įsitraukti į veiklą. Dalyviams dažnai buvo mokama kriptovaliutomis, tai skatino ilgalaikį įsitraukimą ir pritraukė ženklų sekėjų skaičių. Pasitelkiant žaidybinius principus – viešus paminėjimus, lyderių lenteles, virtualius ženkliukus – savanoriams buvo kuriamas svarbos ir pripažinimo jausmas. Ši žaidybinė manipuliacija, nukreipta į jaunesnius asmenis, buvo emociškai stiprinama naratyvu apie „Rusijos gynimą" ar „kerštą" dėl veiklos, nukreiptos prieš Rusiją[61].

[54] GRU 29155 Cyber Actors. (n. d.). Prieiga per internetą: *https://www.fbi.gov/wanted/cyber/gru-29155-cyber-actors*
[55] 2024 Report on the Protection of the Constitution. Brief summary. (n. d.). Prieiga per internetą: *https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2025-06-brief-summary-2024-report-on-the-protection-of-the-constitution.pdf*
[56] Khomenko, I. (2024 m. rugsėjo 9 d.). German Intelligence Accuses Russia of Widespread Cyberattacks on NATO and EU. Prieiga per internetą: *https://united24media.com/latest-news/german-intelligence-accuses-russia-of-widespread-cyberattacks-on-nato-and-eu-2198*
[57] Barkhush, A. (2025 m. birželio 27 d.). MI5 Chief Warns of Russia's Intelligence Plotting "Mayhem" on UK and European Streets. Prieiga per internetą: *https://united24media.com/latest-news/mi5-chief-warns-of-russias-intelligence-plotting-mayhem-on-uk-and-european-streets-2915*
[58] Tarptautinė operacija „Eastwood" – kirtis hakerių grupuotei NoName057(16). (2025 m. liepos 16 d.). Prieiga per internetą: *https://policija.lrv.lt/lt/naujienos/tarptautine-operacija-eastwood-kirtis-hakeriu-grupuotei-noname05716/*
[59] „DDoS" ataka (Distributed Denial of Service) – tai paskirstytas paslaugos blokavimo išpuolis, kurio metu nusikaltėliai užtvindo tinklapius ar serverius dideliu kiekiu piktybinio srauto, siekdami sutrikdyti normalų paslaugų teikimą. Dėl spartaus daiktų interneto (IoT) įrenginių plitimo, nuotolinio darbo ir pažangesnių botnet tinklų, 2025 metais „DDoS" atakos išlieka viena didžiausių kibernetinių grėsmių. Žr.: Vaičiulis, E. (2025 m. gegužės 8 d.). Kas yra DDoS ataka? Prieiga per internetą: *https://itbites.lt/kas-yra-ddos-ataka/*
[60] Tarptautinė operacija „Eastwood" – kirtis hakerių grupuotei NoName057(16). (2025 m. liepos 16 d.). Prieiga per internetą: *https://policija.lrv.lt/lt/naujienos/tarptautine-operacija-eastwood-kirtis-hakeriu-grupuotei-noname05716/*
[61] Ten pat.

NoName057(16) veikimą verta sugretinti su Rusijos kibernetinių nusikaltėlių grupuotė, žinoma kaip *Qilin* (liet. Čilinas, mitologinis kinų vienaragis[62]). *Qilin* veikimo būdas: programišiai užblokuoja kokios nors įmonės failus, kad ši negalėtų funkcionuoti. Gavus išpirką failai „atrakinami". Jei auka delsia sumokėti, *Qilin* ima viešinti pavogtus svarbius duomenis. Nuo 2022 m. spalio 8 d. iki 2025 m. rugpjūčio 3 d. *Qilin* surengė 633 išpuolius visame pasaulyje[63].

Qilin veikia labiau iš komercinių, o ne ideologinių paskatų. Tai yra nelegali išpirkos paslaugų teikėja, parduodanti *RaaS* tipo programą (angl. *Ransomware as a Service*, santrumpa *RaaS*) [64,65]. Toks paslaugų tinklas veikia vadinamajame „tamsiajame internete" (angl. *darknet*)[66]. Besinaudojantieji *Qilin* nelegalia paslauga pasiima iki 85 proc. išpirkos[67].

Qilin patraukė žiniasklaidos dėmesį dėl išpuolio JK. 2024 m. birželio 3 d. mediciniuius tyrimus atliekanti kompanija Synnovis, vykdanti JK Nacionalinės sveikatos tarnybos ligoninių užsakymus, patyrė didelio masto kibernetinę ataką. Dėl šio incidento sutriko dauguma *Synnovis* teikiamų paslaugų[68]. Įsilaužę į sistemą, *Qilin* programišiai užšifravo svarbią informaciją ir ji tapo neprieinama. Spausdami sumokėti išpirką bitkoinais (apie 40 mln. svarų sterlingų), užpuolikai pavogė įslaptintus duomenis, tokius kaip pacientų vardai ir pavardės, gimimo datos ir kraujo tyrimų aprašymai. Negavę išpirkos, užpuolikai ėmė tai viešinti. **Kibernetinė ataka sutrikdė daugiau nei 3 tūkst. vizitų pas bendrosios praktikos gydytojus ir daugiau nei 800 planinių operacijų.** Buvo paveiktos itin svarbios paslaugos, įskaitant vėžio gydymą ir organų transplantaciją. Negalint panaudoti kraujo tyrimų duomenų, iškilo perpylimui reikalingo kraujo deficitas[69].

Apibendrinant galima teigti, kad kibernetinių atakų poveikis gali būti ne mažesnis, nei fizinėmis priemonėmis atlikto sabotažo ar netgi karo veiksmų. Žiniasklaidos pranešimai apie kibernetines atakas didina programišių matomumą, kartu ir įtaką. Internetas (ypač „tamsusis") leidžia sukurti terpę, kurioje programišiai verbuojami ne vien ideologiniais, bet ir komerciniais pagrindais (t. y. kenkėjiškos grupės veikia kaip paslaugų pardavėjos).

4. Lietuvos parengtis hibridinėms grėsmėms

Hibridinės grėsmės Lietuvoje suvokiamos ir įvertintos tiek instituciniu, tiek visuomeniniu lygmenimis. Atsparumo hibridinėms grėsmėms siekis nustatytas kaip Lietuvos užsienio politikos gairė[70]. Krašto

[62] Bloškytė, N. (2015 m. gegužės 19 d.). Čilinas. Prieiga per internetą: *https://azijoszinynas.vdu.lt/kinija-taivanas/cilinas-3/*
[63] Qilin. (2025 m. rugpjūčio 3 d.). Prieiga per internetą: *https://www.ransomware.live/group/qilin*
[64] Lakshmanan, R. (2023 m. gegužės 16 d.). Inside Qilin Ransomware: Affiliates Take Home 85% of Ransom Payouts. Prieiga per internetą: *https://thehackernews.com/2023/05/inside-qilin-ransomware-affiliates-take.html*
[65] Ransomware-as-a-Service (RaaS) Explained. (n. d.). Prieiga per internetą: *https://www.fortinet.com/resources/cyberglossary/ransomware-as-a-service-raas*
[66] Tamsusis internetas (*darknet*) yra užkoduotas interneto tinklas, pasiekiamas tik per specialias programas ir protokolus, užtikrinančius vartotojų anonimiškumą. Jis skiriasi nuo įprasto interneto, nes jo turinio neranda įprastos paieškos sistemos ir naršyklės. *Darknet* gali būti naudojamas įvairiems tikslams, įskaitant anoniminę komunikaciją, failų dalijimąsi ir nusikalstamą veiklą. Žr.: What is the darknet?. (n. d.). Prieiga per internetą: *https://www.myrasecurity.com/en/knowledge-hub/darknet/*
[67] Lakshmanan, R. (2023 m. gegužės 16 d.). Inside Qilin Ransomware: Affiliates Take Home 85% of Ransom Payouts. Prieiga per internetą: *https://thehackernews.com/2023/05/inside-qilin-ransomware-affiliates-take.html*
[68] Understanding the Synnovis Ransomware Attack: Key Insights, Vulnerabilities, and Defence Strategies. (2025 m. kovo 1 d.). Prieiga per internetą: *https://medium.com/@goodycyb/understanding-the-synnovis-ransomware-attack-key-insights-vulnerabilities-and-defence-strategies-7e9fcd464140*
[69] Almost all services back on track after cyber attack hit south east London. (2025 m. spalio 4 d.). Prieiga per internetą: *https://www.england.nhs.uk/london/2024/10/04/almost-all-services-back-on-track-after-cyber-attack-hit-south-east-london/*
[70] Atsparumas hibridinėms grėsmėms siekis Lietuvos užsienio politikoje. (n. d.). Prieiga per internetą: *https://www.urm.lt/lietuvos-saugumo-politika/atsparumo-hibridinems-gresmems-siekis-lietuvos-uzsienio-politikoje/315*

apsaugos ministerijoje (KAM) veikia Atsparumo hibridinėms grėsmėms grupė[71]. Šios grupės vyresnysis patarėjas plk. ltn. Darius Barčius 2024 m. kovą konferencijoje „Verslo vaidmuo gynyboje dieną X. Kuo galėsime prisidėti“[72,73] perspėjo: „Priešiški veikėjai visuomenės atžvilgiu siekia nutraukti sutartį tarp valstybės institucijų ir visuomenės, mažinti visuomenės galimybes kontroliuoti valstybės valdymo procesus, išlaikyti žemą korupcijos suvokimo indeksą ir aukštą neteisingumo lygį. Taip pat sumažinti piliečių dalyvavimą valstybės valdyme ir sumažinti pasitikėjimą.“[74]

Pasak D. Barčiaus, priešiškų jėgų taikiniais Lietuvoje tampa sritys nuo ekonomikos iki kultūros. Jo nuomone, šie 2021 m. įvykiai buvo inspiruoti išorės jėgų:

- socialiniai neramumai COVID-19 pandemijos metu[75],
- padidėjęs nelegalių migrantų skaičius pasienyje su Baltarusija,
- riaušės migrantų apgyvendinimo centruose,
- protestai prieš migrantų integraciją[76].

D. Barčius pateikia pavyzdį: Bangladeše aktyviai platinta socialinė reklama, kurioje trečiųjų šalių gyventojai raginti įsidarbinti Lietuvoje, gauti darbo vizas ir laisvai keliauti po visą ES. Buvo teigiama, kad Lietuvoje visus metus trunka vasara, auga palmės, pragyvenimo lygio (atlyginimų) apatinė riba yra apie 3 tūkst. eurų. Informaciją pastebėjo ne Lietuvos valstybės atstovai, o verslininkas[77].

Toje pačioje konferencijoje kalbėjęs buvęs Valstybės saugumo departamento (VSD) vadovas Gediminas Grina atkreipė dėmesį į infrastruktūros saugumą – pvz., vandens, elektros tiekimą:„Įsivaizduokite, Vilniuje 600 tūkst. gyventojų. Tai čia nereikia jokių tankų, užtenka trims dienoms sutrikdyti vandens tiekimą ir greitai pamatysite, kas čia bus. Čia, mano supratimu, yra pagrindinės hibridinės grėsmės, o ne kas ten feisbuke ką rašinėja.“[78]

Panašių įžvalgų Vilniuje 2025 m. birželį vykusioje konferencijoje *Energy Forum* pateikė NATO Energetinio saugumo kompetencijos centro ekspertė, Lietuvos užsienio reikalų ministerijos diplomatė Kristina Rimkūnaitė. Ji kalbėjo apie elektros energijos tiekimo nutraukimo atvejus Europoje[79]. Diplomatė priminė tris nesenus incidentus:

---

[71] Atsparumo hibridinėms grėsmėms grupė. (n. d.). Prieiga per internetą: *https://www.lrvalstybe.lt/kontaktai/atsparumo-hibridinems-gresmems-grupe-20505*
[72] Verslo vaidmuo gynyboje dieną X. Kuo galėsime prisidėti. (n. d.). Prieiga per internetą: *https://www.lrs.lt/sip/getFile3?p_fid=73836*
[73] Diskusija „Verslo vaidmuo gynyboje dieną X. Kuo galėsime prisidėti?“ (2024 m. kovo 7 d.). Prieiga per internetą (vaizdo įrašas): *https://www.youtube.com/live/lwgow07toTw?si=2zlCGmbg0lllE4Yo*
[74] Narkūnas, V. (2024 m. kovo 23 d.). Grina apie hibridines grėsmes: nereikia nė tankų, įsivaizduokite, jei Vilniui trims dienoms atjungtų vandenį. Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/2220420/grina-apie-hibridines-gresmes-nereikia-ne-tanku-isivaizduokite-jei-vilniui-trims-dienoms-atjungtu-vandeni*
[75] Jakučionis, S., Masiokaitė-Liubinienė, A. (2021 m. rugpjūčio 11 d.). Svarbiausios trečiadienio naujienos: reakcijos į riaušes prie Seimo ir ribojimai neturintiems imuniteto nuo COVID-19. Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/1467173/svarbiausios-treciadienio-naujienos-reakcijos-i-riauses-prie-seimo-ir-ribojimai-neturintiems-imuniteto-nuo-covid-19*
[76] Narkūnas, V. (2024 m. kovo 23 d.). Grina apie hibridines grėsmes: nereikia nė tankų, įsivaizduokite, jei Vilniui trims dienoms atjungtų vandenį. Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/2220420/grina-apie-hibridines-gresmes-nereikia-ne-tanku-isivaizduokite-jei-vilniui-trims-dienoms-atjungtu-vandeni*
[77] Ten pat.
[78] Ten pat.
[79] Pepcevičiūtė, I. (2025 m. birželio 9 d.). Kristina Rimkūnaitė – apie hibridines ir kibernetines grėsmes energetikos infrastruktūrai: kaip gali paveikti mūsų gyvenimą. Prieiga per internetą: *https://www.delfi.lt/projektai/energy-forum-2025/kristina-rimkunaite-apie-hibridines-ir-kibernetines-gresmes-kokia-galima-itaka-gynybai-baltijos-juros-regione-120115622*

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

- elektros tiekimo nutrūkimas Londono Heathrow oro uoste 2025 m. kovo mėn., kuris palietė maždaug 270 tūkst. keleivių[80],
- elektros tiekimo nutrūkimas Pietų Prancūzijoje, Portugalijoje ir Ispanijoje 2025 m. balandžio mėn.[81],
- Londono metro eismo sutrikimas dėl elektros dingimo 2025 m. gegužės mėn., kai piko valandą visas pagrindinės linijos buvo sustabdytos[82].

Socialiniai hibridinių grėsmių aspektai ne mažiau svarbūs nei techniniai. Generolo Jono Žemaičio Lietuvos karo akademijos Saugumo politikos grupės profesorius Giedrius Česnakas konferencijoje „Verslo vaidmuo gynyboje dieną X. Kuo galėsime prisidėti?" teigė, kad Lietuvos sąlygomis atsparumo hibridinėms grėsmėms tinklas biurokratiškai yra sudėliotas gražiai, tačiau pasigendama konkretumo ir aiškumo[83].

G. Česnakas priminė tokius socialiai reikšmingus dalykus kaip kovą su korupcija, greitą sprendimų priėmimą, duomenų apsaugos užtikrinimą. Jo nuomone, politinio elito ir visuomenės susipriešinimas, kurio būtina išvengti, sukuria puikią terpę priešui destabilizuoti savo taikinį: Ukrainoje 2014-aisiais visuomenė ir politinis elitas buvo susipriešinę ir tai sukūrė puikią galimybę Krymo aneksijai[84].

Šioje konferencijoje G. Grina pabrėžė piliečių apginklavimo reikšmę: „Jeigu priešas žinotų, kad Lietuvoje yra kokie 300 tūkst. ginkluotų žmonių automatais, tai labai gerai pagalvotų, ar čia verta kišti nosį. <...> Aišku, yra kitos problemos, kur tuos ginklus laikyti, bet suprantate, čia yra išvestiniai dalykai."[85]

Vargu ar hibridiniais veiksmais galima imituoti karinį antpuolį prieš Lietuvą ar stichinę nelaimę kaimyninėje šalyje (pvz. Baltarusijoje), tačiau Lietuvos parengtis tokioms grėsmėms šiuo metu kelia daug klausimų. 2025 m. gegužę pristatyto Vilniaus evakuacijos plano komentarai:

„Vilniuje pristačius evakuacijos planą, atrodo, atsivėrė Pandoros skrynia. Aplinkinių rajonų merai ėmė vardyti kelius, kuriuos būtina tvarkyti, jei tektų evakuoti gyventojus, kitaip – jie tiesiog įstrigtų. Susisiekimo ministras sako, evakuacijos keliai bus tvarkomi, tačiau kad jie neužsikimštų į vieną pusę važiuojant daugumai gyventojų – neįmanoma. Klausimas – ne tik kaip išvykti, bet ir kur reikėtų vykti". [86]

„Pagal Vilniaus planą – prasidedant karui, evakuacija vyktų Panevėžio, Šiaulių kryptimis, nors judėti Suvalkų koridoriaus link gali būti nesaugu, numatyta ir Alytaus kryptis. Gresiant kitoms nelaimėms – pavyzdžiui galingai stichijai – numatyta, kad vilniečiai galėtų vykti Klaipėdos link"[87].

---

[80] 'Catastrophic failure' led to Heathrow power outage - with chances missed to prevent it. (2025 m. liepos 2 d.). Prieiga per internetą: *https://news.sky.com/story/catastrophic-failure-that-led-to-heathrow-power-outage-revealed-as-report-outlines-the-chances-missed-to-prevent-it-13391266*

[81] Prancūzijoje, Ispanijoje ir Portugalijoje – dideli elektros tiekimo sutrikimai. (2024 m. balandžio 28 d.). Prieiga per internetą: *https://www.vz.lt/energetika/2025/04/28/prancuzijoje-ispanijoje-ir-portugalijoje-dideli-elektros-tiekimo-sutrikimai-567073*

[82] Power failures cause disruption on London Tube. (2025 m. gegužės 12 d.). Prieiga per internetą: *https://www.reuters.com/world/uk/power-failures-cause-london-tube-suspensions-2025-05-12/*

[83] Narkūnas, V. (2024 m. kovo 23 d.). Grina apie hibridines grėsmes: nereikia nė tankų, įsivaizduokite, jei Vilniui trims dienoms atjungtų vandenį. Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/2220420/grina-apie-hibridines-gresmes-nereikia-ne-tanku-isivaizduokite-jei-vilniui-trims-dienoms-atjungtu-vandeni*

[84] Ten pat.

[85] Narkūnas, V. (2024 m. kovo 23 d.). Grina apie hibridines grėsmes: nereikia nė tankų, įsivaizduokite, jei Vilniui trims dienoms atjungtų vandenį. Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/2220420/grina-apie-hibridines-gresmes-nereikia-ne-tanku-isivaizduokite-jei-vilniui-trims-dienoms-atjungtu-vandeni*

[86] Valiauskaitė, A. (2025 m. gegužės 4 d.). Vilniaus evakuacijos planas atvėrė Pandoros skrynią – ne tik kaip, bet ir kur vykti? Prieiga per internetą: *https://www.lrt.lt/naujienos/lietuvoje/2/2552755/vilniaus-evakuacijos-planas-atvere-pandoros-skrynia-ne-tik-kaip-bet-ir-kur-vykti*

[87] Ten pat.

Atsispiriant hibridinėms grėsmėms akcentuotina būtent socialinių veiksnių reikšmė. Šioje apžvalgoje aptarti Rusijos hibridiniai veiksmai Europoje kol kas reiškiasi kaip gana riboto masto diversijos. Verta atkreipti dėmesį, kad gyventojų panika gali būti sukelta būtent hibridinėmis priemonėmis – skleidžiant dezinformaciją. Nors valstybės institucijos bent jau planų lygmeniu transliuoja žinią apie pasirengimą karui, taip pat ir hibridiniam, daugelis pavienių piliečių neturi jokios veiksmų programos karo atveju. Krizės sąlygomis būtent valstybės komunikacinės klaidos gali padaryti neigiamą poveikį situacijos raidai.

5. ES priemonės prieš hibridinius veiksmus, NATO sutarties 5 straipsnio taikymas

Nuo 2016 m. Europos Vadovų Taryba ir Europos Sąjungos Taryba rengia dokumentus ir priemonių planus, skirtus hibridinių grėsmių pavojui[88].

Nors **pagrindinė atsakomybė už kovą su hibridinėmis grėsmėmis tenka atskiroms ES narėms**, jos koordinuoja veiksmus, siekdamos kolektyviai atsispirti tokiems iššūkiams. Nuo 2017 m. Helsinkyje veikia Europos kovos su mišriomis grėsmėmis kompetencijos centras[89,90]. 2024 m. gegužės mėn. ES Taryba patvirtino ES greitojo reagavimo į hibridines grėsmes grupių praktinio sudarymo orientacinę sistemą[91].

2024 m. spalio 8 d. ES įteisino sankcijų sistemą asmenims ir subjektams, atsakingiems už destabilizuojančią veiklą prieš ES ir jos nares[92]. Šiuo metu sankcijos, kurios apima bankų sąskaitų įšaldymą ir draudimą finansuoti taikomos 15 organizacijų ir 47 asmenims (pastariesiems draudžiama įvažiuoti į ES). Į skaičių įeina ir 2025 m. liepos 15 d. sprendimu į sąrašą įtraukti 9 fiziniai ir 6 juridiniai asmenys[93]. Tarp tądien sankcionuotų organizacijų, pvz., paminėtas Rusijos Baltijos laivyno 841-asis atskiras elektroninio karo centras (angl. *841st Separate Electronic Warfare Center of the Baltic Fleet*)[94], Rusijos televizijos ir radijo transliavimo tinklas, veikiantis okupuotose Ukrainos teritorijose (angl. *Russian Television and Radio Broadcasting Network*, rus. *Российская телевизионная и радиовещательная сеть*)[95], BRICS šalių žurnalistų asociacijai (angl. *BRICS Journalists Association*)[96].

Kiek anksčiau ES nustatė ribojamąsias priemones Nathalie Yamb[97] – socialinių tinklų nuomonės formuotojai ir atvirai Rusijos rėmėjai, kuri perėmė Maskvos propagandos kalbą, nukreiptą prieš Vakarus ir ypač Prancūziją. N. Yamb

[88] Hibridinės grėsmės. (n. d.). Prieiga per internetą: *https://www.consilium.europa.eu/lt/policies/hybrid-threats/*
[89] Hybrid CoE. (n. d.). Prieiga per internetą: *https://www.hybridcoe.fi/*
[90] Helsinkyje veiklą pradėjo Europos kovos su mišriomis grėsmėmis kompetencijos centras. (2017 rugsėjo 7 d.). Prieiga per internetą: *https://www.15min.lt/naujiena/aktualu/pasaulis/helsinkyje-veikla-pradejo-europos-kovos-su-misriomis-gresmemis-kompetencijos-centras-57-850274*
[91] Hibridinės grėsmės. Taryba atvėrė kelią greitojo reagavimo į hibridines grėsmes grupių dislokavimui. (2024 m. gegužės 21 d.). Prieiga per internetą: *https://www.consilium.europa.eu/lt/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/*
[92] ES sankcijos Rusijai. (n. d.). Prieiga per internetą: *https://www.consilium.europa.eu/lt/policies/sanctions-against-russia/#hybrid*
[93] Russian hybrid threats: EU lists nine individuals and six entities responsible for destabilising actions in the EU and Ukraine. (2025 m. liepos 15 d.). Prieiga per internetą: *https://www.consilium.europa.eu/en/press/press-releases/2025/07/15/russian-hybrid-threats-eu-lists-nine-individuals-and-six-entities-responsible-for-destabilising-actions-in-the-eu-and-ukraine/*
[94] 841st Separate Electronic Warfare Center of the Baltic Fleet. (n. d.). Prieiga per internetą: *https://www.opensanctions.org/entities/NK-4R9xdDotjgvec9URYfiFBB/*
[95] Federal State-owned Enterprise „Russian Television and Radio Broadcasting Network". (n. d.). Prieiga per internetą: *https://www.opensanctions.org/entities/NK-mq9ddT6xZ7GkxGiwM5mjM6/*
[96] BRICS Journalist Association. (n. d.). Prieiga per internetą: *https://www.opensanctions.org/entities/NK-Co7wMkKRyHeLqmnYqaXkWY/*
[97] Nathalie Yamb. (n. d.). Prieiga per internetą: *https://www.nathalieyamb.com/*

palaiko konkrečius ryšius su AFRIC – organizacija, susijusia su Rusijos privačiomis karinėmis struktūromis ir yra atsakinga už Rusijos Federacijos rėmimą manipuliuojant informacija[98].

Europos politikos analizės centro (*Center for European Policy Analysis*, CEPA) Vašingtone vizituojantis bendradarbis, diplomatas Eitvydas Bajarūnas Lietuvos žiniasklaidoje rašė apie ES ir Lietuvos galimybes atsispirti hibridinėms grėsmėms[99,100]. CEPA tinklalapyje E. Bajarūnas svarstė apie sąlygas, kuriomis NATO galėtų pritaikyti Aljanso sutarties 5 straipsnį atsakant į hibridines grėsmes[101]. Diplomatas vardijo galimus NATO atsakomuosius veiksmus:

- galingos kibernetinės atakos, kurios sutrikdytų svarbią Rusijos infrastruktūrą, pavyzdžiui, elektros tinklus, finansų sistemas ar karinius tinklus;
- kritinės infrastruktūros sabotažas: turto, pvz., povandeninių kabelių, vamzdynų ar transporto tinklų, sunaikinimas ar sutrikdymas, ypač jei tai daro didelį poveikį nacionaliniam saugumui;
- saugumo priemonės jūroje, įskaitant užsienio laivų sustabdymą ir patikras, draudimo dokumentų galiojimo tikrinimą ir įtartinų laivų sulaikymą; kraštutiniais atvejais NATO galėtų įgyvendinti jūrų blokadą[102].

E. Bajarūnas detaliau nušviečia aplinkybes, kuriomis NATO galiausiai pritaikytų Aljanso 5 straipsnį esant hibridinėms grėsmėms:

- Jeigu siekiant destabilizuoti NATO šalį Rusija vykdo plataus spektro koordinuotas hibridines operacijas, pvz., vienu metu derina dezinformaciją, ekonominę prievartą, kibernetines atakas. Aljansas galėtų dislokuoti tiek įprastines, tiek kovos su hibridiniais pavojais pajėgas, siekdamas atkurti stabilumą, apsaugoti kritinę infrastruktūrą ir atgrasyti nuo tolesnių išpuolių. Tai būtų reagavimo į ekstremalias situacijas pajėgos, įskaitant žvalgybos ir saugumo padalinius. Aljansas taip pat galėtų dislokuoti karinius dalinius nukentėjusioje šalyje, kad atgrasytų nuo tolesnės agresijos ir pademonstruotų vieningą atsaką.
- Rusijai taikant hibridinę taktiką, kuria siekiama pakenkti NATO šalies suverenitetui destabilizuojant jos vyriausybę arba manipuliuojant rinkimais, Aljansas galėtų dislokuoti įprastines pajėgas ir žvalgybos padalinius bei padėti užtikrinti rinkimų ir vyriausybinių institucijų saugumą. Priemonės galėtų apimti kibernetinio saugumo ir žiniasklaidos infrastruktūros stiprinimą, siekiant kovoti su dezinformacija ir manipuliavimu.
- Rusijos išpuolis prieš dislokuotas NATO pajėgas, nepriklausomai nuo metodo, paskatintų kolektyvinį karinį ir politinį atsaką. Tai galėtų apimti kibernetinės gynybos priemones, gausesnį kariuomenės dislokavimą ir atsakomuosius smūgius.

---

[98] Russian hybrid threats: EU lists nine individuals and six entities responsible for destabilising actions in the EU and Ukraine. (2025 m. liepos 15 d.). Prieiga per internetą: *https://www.consilium.europa.eu/en/press/press-releases/2025/07/15/russian-hybrid-threats-eu-lists-nine-individuals-and-six-entities-responsible-for-destabilising-actions-in-the-eu-and-ukraine/*

[99] Bajarūnas, E. (2024 m. lapkričio 20 d.). Perkelkime hibridinį karą į Rusiją. Prieiga per internetą: *https://www.15min.lt/naujiena/aktualu/komentarai/eitvydas-bajarunas-perkelkime-hibridini-kara-i-rusija-500-2346136*

[100] Bajarūnas, E. (2025 m. birželio 2 d.). Kaip atgrasyti Rusiją: apie hibridines grėsmes ir šešėlinį karą. Prieiga per internetą: *https://www.lrt.lt/naujienos/nuomones/3/2578405/eitvydas-bajarunas-kaip-atgrasyti-rusija-apie-hibridines-gresmes-ir-seselini-kara*

[101] Bajarūnas, E. (2025 m. vasario 11 d.). Using NATO's Article 5 Against Hybrid Attacks. Prieiga per internetą: *https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/*

[102] Bajarūnas, E. (2025 m. vasario 11 d.). Using NATO's Article 5 Against Hybrid Attacks. Prieiga per internetą: *https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/* .

- Rusijai vykdant išpuolius prieš NATO infrastruktūrą (net ir hibridinėmis priemonėmis), pavyzdžiui, karines bazes ar ryšių sistemas, NATO galėtų nuspręsti, kad tokioms netradicinėms priemonėms dabar taikomas 5 straipsnis.

Prieš Rusiją nukreipto hibridinio veiksmo pavyzdys (nors jokia NATO valstybė dėl to neprisiėmė atsakomybės) yra 2025 m. liepos 28 d. Ukrainą ir Baltarusijos opoziciją remiančių programišių kibernetinė ataka prieš Rusijos oro bendrovę *Aeroflot*. Vien tą dieną bendrovė atšaukė 42 proc. skrydžių, tai palietė 20 tūkst. žmonių. Skaičiuojama, kad *Aeroflot* nuostoliai siekia apie 50 mln. USD ir sugadintoms duomenų sistemoms atkurti prireiks maždaug vienerių metų[103, 104].

Eskaluojant ES ir NATO gynybos nuo hibridinių grėsmių priemones, kritinė riba yra Aljanso sutarties 5 straipsnio aktyvavimas. Po to konfrontuojančios šalys žengia arčiau atviro karo. Veikimas pagal 5 straipsnį suteiktų NATO įgaliojimus panaudoti visas būtinas priemones, įskaitant karinę jėgą. Tai būtų paskutinė priemonė, kurios imamasi tik tada, kai išnaudotos visos kitos galimybės, o jos įgyvendinimui reikėtų visų NATO narių sutikimo.

7. Apibendrinimas ir akcentai, į ką atkreipti dėmesį ateityje

Hibridinių Rusijos išpuolių skaičius Europoje nuo 2022 m. (3 išpuoliai) iki 2024 m. (34 išpuoliai) išaugo daugiau nei 10 kartų. IISS duomenimis, 2025 m. sausį-gegužę būta 11 išpuolių. Nors Rusija naudoja gyvybei ir turtui pavojingas priemones, veiksmų mastas kol kas verčia manyti, kad Maskva labiau siekia atgrasyti nuo ginklų siuntimo ir kitokios pagalbos Ukrainai, o ne padaryti reikšmingą žalą. Iki šiol per išpuolius nukentėjo santykinai nedaug žmonių ir tai rodo, kad Rusija veikia su mažomis sąnaudomis bei tikimybe paneigti savo dalyvavimą. Vis dar žemas smurto lygis leidžia Maskvai prireikus eskaluoti teroristinius veiksmus iki didesnio masto kampanijos.

Kibernetinių atakų poveikis gali būti ne mažesnis, nei fizinėmis priemonėmis atlikto sabotažo ar netgi karo veiksmų. Žiniasklaidos pranešimai apie kibernetines atakas didina programišių matomumą, kartu ir įtaką. Internetas (ypač „tamsusis“) leidžia sukurti terpę, kurioje programišiai verbuojami ne vien ideologiniais, bet ir komerciniais pagrindais (t. y. kenkėjiškos grupės veikia kaip paslaugų pardavėjos).

Eskaluojant ES ir NATO gynybos nuo hibridinių grėsmių priemones, kritinė riba yra Aljanso sutarties 5 straipsnio aktyvavimas. Po to konfrontuojančios šalys žengia arčiau atviro karo. Veikimas pagal 5 straipsnį suteiktų NATO įgaliojimus panaudoti visas būtinas priemones, įskaitant karinę jėgą. Tai būtų paskutinė

[103] Išpuolį prieš „Aeroflot“ įvykdę programišiai: „Šlovė Ukrainai! Tegyvuoja Baltarusija!“. (2025 m. liepos 28 d.). Prieiga per internetą: *https://www.lrt.lt/naujienos/mokslas-ir-it/11/2627147/ispuoli-pries-aeroflot-ivykde-programisiai-slove-ukrainai-tegyvuoja-baltarusija*
[104] Afonina, S. (2025 m. liepos 29 d.). Aeroflot's losses due to the cyberattack are estimated at up to $50 million, with a recovery period of about a year. Prieiga per internetą: *https://biz.liga.net/en/all/transport/novosti/aeroflots-losses-due-to-the-cyberattack-are-estimated-at-up-to-50-million-with-a-recovery-period-of-about-a-year*

priemonė, kurios imamasi tik tada, kai išnaudotos visos kitos galimybės, o jos įgyvendinimui reikėtų visų NATO narių sutikimo.

Verta atkreipti dėmesį, kad gyventojų panika gali būti sukelta būtent hibridinėmis priemonėmis – skleidžiant dezinformaciją. Nors Lietuvos valstybės institucijos bent jau planų lygmeniu transliuoja žinią apie pasirengimą karui, taip pat ir hibridiniam, daugelis pavienių piliečių neturi jokios veiksmų programos. Krizės sąlygomis būtent valstybės komunikacinės klaidos gali padaryti labai neigiamą poveikį situacijos raidai.

Akcentai, į ką atkreipti dėmesį ateityje:

- Lietuvos viešojoje erdvėje apstu signalų apie pavienių institucijų pasirengimą ekstremalioms situacijoms, tačiau stokojama visuomenei prieinamos informacijos apie kompleksinę valstybės parengtį.

- Būtina plėtoti krizėms skirtą gyventojų informavimo sistemą mobiliuoju ryšiu, kuri apimtų visą šalį (lokaliai veikiančios priemonės pavyzdys yra nuo 2025 m. liepos pabaigos Vilniuje veikianti programėlė „Kovas"[105])

- Informacijoje apie gyventojų pasirengimą karui vardijami išgyvenimui būtini daiktai, maisto atsargos, kurie reikalingi tiek evakuojantis, tiek nekeičiant buvimo vietos. Evakuacija yra pagrindinis tokios informacijos fonas. Scenarijus, kai nemaža dalis gyventojų pasilieka karo veiksmų zonoje, kadangi neturi galimybės evakuotis, šiuo metu beveik neaptariamas, nors, pvz., galimybės nebuvimas ar nenoras evakuotis yra karo Ukrainoje realija.

[105] Vilnius pristato aplikaciją „Kovas" – tiesiogiai informuos gyventojus apie išskirtines situacijas mieste. (2025 m. liepos 24 d.). Prieiga per internetą: *https://vilnius.lt/naujienos/vilnius-pristato-aplikacija-kovas-tiesiogiai-informuos-gyventojus-apie-isskirtines-situacijas-mieste*

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