

Biuletenio tematika ir tema

Tarptautiniai santykiai ir geopolitika

Biuletenio laidos antraštė, probleminis klausimas Dirbtinio intelekto revoliucija karyboje

Esminiai žodžiai

Kariniai konfliktai, dirbtinis intelektas, JAV, Izraelis, *Palantir*, *Anthropic*, Microsoft, *Lavender*, *Gospel*, *Azure*

Serija ir registracijos numeris

ZD-2026-5

Leidimo data

2026-06-05

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

2010-05-05 -
2026-06-01

Šaltiniai: kalbos

- Lietuvių k. Lenkų k.
 Anglų k. Kitos ES kalbos
 Rusų k. Kitos

Citavimui (APA stiliumi)

Nacionalinė biblioteka, Informacijos analitikos skyrius (2026). *Dirbtinio intelekto revoliucija karyboje* (ZD-2026-5). Vilnius.

Kontaktiniai duomenys

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

Turinio apžvalga

Aptariama DI integracija į ginkluotųjų pajėgų valdymą:

- *Palantir* ir kitų technologijų kompanijų vaidmuo Ukrainoje;
- DI taikymas Izraelio karinėse operacijose;
- etiniai klausimai dėl DI karinio panaudojimo.

1. Įžanga


Šioje apžvalgoje nušviečiamas dirbtinio intelekto (DI) naudojimas karyboje. Tai dinamiškas, greitai besiplėtojantis reiškinys, kuriam tinka **revoliucijos** apibūdinimas.

DI jau suteikia esminį karinį pranašumą, ir tikėtina, ateityje ginklavimosi varžybų rezultatus nulems būtent šių technologijų plėtra. Pateikiama DI integravimo į Jungtinių Amerikos Valstijų (JAV), Ukrainos ir Izraelio karines sistemas pavyzdžių.

Darbe nemažai vietos skirta JAV bendrovei *Palantir Technologies*, kurios generalinis direktorius Alexas Karpas mano, kad atgrasymo srityje DI keičia branduolinį ginklą.

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

Cituojant arba naudojant šį šaltinį, nuoroda į Nacionalinę biblioteką yra būtina.
Šioje apžvalgoje pateikiamas turinys nėra oficiali Nacionalinės bibliotekos nuomonė.

LNB / IAS / ZD / 2026-06-05 / Psl. 1 iš 14
© Nacionalinė biblioteka, 2026 /  Слава Україні!

Pasak Karpo, branduolinio atgrasymo amžius baigiasi, jį keičia DI paremta atgrasymo era. Jis teigia, kad pagrindinis klausimas yra ne tai, ar bus sukurti ginklai su integruotu DI, o tai, kas juos sukurs pirmas. Jis ragina JAV Silicio slėnio technologijų kompanijas teikti pirmenybę nacionaliniam saugumui, o ne etinėms diskusijoms dėl DI taikymo moralumo. Karpas DI programinę įrangą laiko „kietąja galia“. Jis įsitikinęs, kad DI turi būti pasitelkiamas siekiant užsitikrinti neįveikiamą JAV ir visų Vakarų dominavimą priimant sprendimus mūsų lauke¹.

Palantir padalinys šiuo metu veikia ir Lietuvoje². Lietuvos Respublikos krašto apsaugos ministerija su šia kompanija ėmė bendradarbiauti 2023 m.

Ta proga cituotas jos vadovas. „Esant dabartinei mūsų geopolitikos trajektorijai, Lietuvos vaidmuo pasaulio arenoje tik didės, – teigia Alexas C. Karpas³, vienas iš „Palantir Technologies Inc.“ įkūrėjų. – Esame labai dėkingi Lietuvos prezidentui už mūsų naują partnerystę su Krašto apsaugos ministerija steigiant techninį centrą Vilniuje. Tai sustiprins ne tik valstybę ir jos Baltijos partneres, bet ir demokratines vertybes, kurias šios šalys siekia įtvirtinti.“⁴

2025 m. kompanija *Palantir* paminėta pranešime apie Dirbtinio intelekto kompetencijų ir technologijų centro steigimą Lietuvoje.

Pranešime rašoma, kad Europos Komisija skyrė finansavimą LitAI – DI kompetencijų ir technologijų centrui. 2025 m. birželio 27 d. Vilniaus universitetas su Ekonomikos ir inovacijų ministerija pasirašė susitarimą dėl ketinimų steigti minėtą centrą. „Šio ambicingo projekto konsorciumą, be akademinės bendruomenės ir verslo atstovų, sudaro ir Valstybės duomenų agentūra [VDA] – pagrindinis partneris, atsakingas už nacionalinių duomenų išteklių valdymą, prieigą ir saugą. <...> LitAI plėtros branduolys – Valstybės duomenų ežeras, „Palantir Foundry“ pagrindu veikianti platforma, kurią VDA kuria ir prižiūri nuo 2023 m. Ši infrastruktūra jau sujungė beveik 500 valstybinių informacinių sistemų, sudarė per 900 viešai prieinamų struktūrinių lentelių ir atvėrė 238 aukštos vertės duomenų rinkinius (HVD). Dar 45 saugios nuotolinės tyrimų aplinkos 2023 m. suteikė mokslininkams bei institucijoms galimybę dirbti su jautriais sveikatos, energetikos ar transporto duomenimis nepažeidžiant jų konfidencialumo.“⁵

Į Lietuvą ketinama perkelti *Palantir* karybos patirtį Ukrainoje. 2026 m. birželio 1–2 d. Vilniuje įvyko antrasis NATO ir Ukrainos gynybos inovatorių forumas, kurį surengė Lietuvos Respublikos krašto apsaugos ministerija kartu su Ukrainos Vyriausybės gynybos inovacijų platforma *Brave 1* (pastaroji sukurta bendradarbiaujant su *Palantir*⁶). Dalyvaujant Lietuvos ir Ukrainos ministrėms pirmininkėms Ingai Ruginienei ir Julijai Svirydenko pasirašytas ketinimų protokolai dėl *BRAVE Lithuania* programos sukūrimo⁷.

Vis dėlto, pasaulio viešojoje erdvėje intensyviai diskutuojama dėl DI keliamo pavojaus pamatinėms žmogaus teisėms⁸.

¹ Vallance, C., Cress L. (2026 m. balandžio 25 m.). The viral manifesto of 'anti-woke' tech boss with NHS and defence contracts. Prieiga per internetą: <https://www.bbc.com/news/articles/c4gjkj7975po>

² Palantir Technologies Lithuania, UAB. (n. d.). Prieiga per internetą: https://rekvizitai.vz.lt/imone/palantir_technologies_lithuania/

³ Pilnas vardas: Alexander Caedmon Karp

⁴ Į Lietuvą įžengs JAV programinės įrangos gigantė „Palantir Technologies“ – bendradarbiaus su Krašto apsaugos ministerija. (2023 m. balandžio 25 d.). Prieiga per internetą: <https://www.lrt.lt/naujienos/verslas/4/1970150/i-lietuva-izengs-jav-programines-irangos-gigante-palantir-technologies-bendradarbiaus-su-krasto-apsaugos-ministerija>

⁵ Valstybės duomenų agentūra – strateginis partneris kuriant Lietuvos dirbtinio intelekto kompetencijų ir technologijų centrą. (2025 m. spalio 10 d.). Prieiga per internetą: <https://vda.lrv.lt/lt/naujienos/valstybes-duomenu-agentura-strateginis-partneris-kuriant-lietuvos-dirbtinio-intelektu-kompetenciju-ir-technologiju-centra-SkL/>

⁶ Ukraine Launches Brave1 Dataroom with Palantir to Train AI Models Using Battlefield Data. (2026 m. sausio 20 d.). Prieiga per internetą: <https://digitalstate.gov.ua/news/tech/ukraine-launches-brave-1-dataroom-with-palantir-to-train-ai-models-using-battlefield-data>

⁷ Lietuva ir Ukraina pasirašė ketinimų protokolą dėl „BRAVE Lithuania“ programos sukūrimo. (2026 m. birželio 1 d.). Prieiga per internetą: <https://kam.lt/lietuva-ir-ukraina-pasirase-ketiniu-protokola-del-brave-lithuania-programos-sukurimo/>

⁸ Skaidra Trilupaitytė: prarandame savo žmogiškąją laisvę patys to neįsąjaujami. (2025 m. birželio 12 d.). Prieiga per internetą: <https://www.lrt.lt/naujienos/kultura/12/2588766/skaidra-trilupaityte-prarandame-savo-zmogiskaja-laisve-patys-to-nejausdami>

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

Antai *Palantir Technologies* jau dešimtmetį bendradarbiauja su JAV Imigracijos ir muitinės tarnyba (angl. *Immigration and Customs Enforcement, ICE*) teikdama duomenų analizės ir DI platformas, skirtas imigracijos stebėsenai ir deportacijai⁹.

Šiuo metu DI vystymo srityje vienaip ar kitaip konkuruoja visos technologijų gigantės, vadinamosios *Big Tech* bendrovės. Daugelis jų siekia valstybinių užsakymų. Apžvalgoje minimas etinis ginčas tarp JAV valstybinės administracijos ir kompanijos *Anthropic*, kurios programos panaudotos Jungtinių Valstijų karinei operacijai Irane, taip pat panašios kolizijos, privertusios bendrovės *Google* ir *Microsoft* pasitraukti iš kai kurių JAV ir Izraelio karinių bei žvalgybinių programų (taikinių nustatymo sistemų *Gospel* ir *Lavender* bei debesijos platformos *Azure* naudojimas karybos ir žvalgybos tikslams Izraelyje sukėlė tarptautinius protestus). Apžvalgoje pateikta medžiaga leidžia kelti klausimą dėl didėjančios valstybių priklausomybės nuo DI plėtojančių kompanijų, kurių poveikis yra sisteminis ir pranoksta įprastos ginkluotės gamintojų įtaką.

Būtina pažymėti, kad popiežius Leonas XIV savo pirmąją encikliką, pasirašytą 2026 m. gegužės 15 d., skyrė būtent DI klausimams¹⁰.

Enciklikoje „Nuostabioji žmonija“ (lot. „Magnifica Humanitas“) popiežius įspėja apie lenktynes „dėl vis galingesnių algoritmų ir didesnių duomenų rinkinių, kurias skatina noras užtikrinti geopolitinį ar komercinį dominavimą“.¹¹

Pristatant encikliką spaudos konferencijoje kartu su popiežiumi dalyvavęs vienas iš kompanijos *Anthropic* įkūrėjų Chrisas Olahas pareiškė, kad „DI keliami klausimai pranoksta pačią su DI dirbančią mokslininkų bendruomenę ne tik savo pasekmėmis, bet ir prigimtimi“¹².

Jau pasigirdo balsų, kad DI kūrėjų ir Vatikano suartėjimas neturėtų švelninti tolimesnių diskusijų dėl su DI susijusių pavojų¹³, kylančių ir iš kol kas menkai varžomo DI taikymo įvairiose saugumo srityse bei karyboje.

2. Prieštaras kompanijos *Palantir* manifestas

Palantir veikimo būdas pasižymi tuo, kad bendrovė neturi didelių skrupulų dėl jos produktų taikymo, ir savo nuostatas, kurioms nestinga įtaigumo, deklaruoja viešai.

Palantir Technologies yra 2003 m. įsteigta programinės įrangos įmonė, kurios specializacija – didžiųjų duomenų (angl. *big data*) analizė. Denveryje, JAV Kolorado valstijoje, įsikūrusios *Palantir* veiklos istorija siekia darbą su elektroninių mokėjimų platforma *PayPal*, konkrečiau – jos sistemomis, skirtomis aptikti neteisėtus veikas, kurios įkvėpė *Palantir* steigėjus kurti programinę įrangą, gebančią atpažinti įtartinus modelius nepažeidžiant privatumo.

⁹ Bhuiyan, J. (2025 m. rugsėjo 22 d.). Documents offer rare insight on Ice's close relationship with Palantir. Prieiga per internetą: <https://www.theguardian.com/us-news/ng-interactive/2025/sep/22/ice-palantir-data>

¹⁰ Camosy, C. (2026 m. gegužės 25 d.). Leono XIV enciklika pasirodo pačiu laiku: dirbtinis intelektas kelia klausimų, į kuriuos atsakyti gali tik religija. Prieiga per internetą: <https://www.bernardinai.lt/leono-xiv-enciklika-pasirodo-paciu-laiku-dirbtinis-intelektas-kelia-klausimu-i-kuriuos-atsakyti-gali-tik-religija/>

¹¹ Popiežius ragina „nuginkluoti“ dirbtinį intelektą. (2026 m. gegužės 25 d.). Prieiga per internetą: <https://www.lrt.lt/naujienos/mokslas-ir-it/11/2939179/popiezius-ragina-nuginkluoti-dirbtini-intelektu>

¹² „Anthropic“ bendrakūrėjas: mums reikia matančiųjų tai, ko nematome mes. (2026 m. gegužės 26 d.). Prieiga per internetą: <https://www.vaticannews.va/lt/eclist.magnifica-humanitas-2026.html>

¹³ Mansoor, S. (2026 m. gegužės 30 d.). Anthropic's alliance with pope on AI harms: all in good faith or 'Vatican-washing?'. Prieiga per internetą: <https://www.theguardian.com/technology/2026/may/30/pope-leo-anthropic-ai>

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

Laikui bėgant, *Palantir* plėtėsi į komercines rinkas, pritaikydama savo platformą įvairioms sritims – nuo tiekimo grandinių iki sveikatos priežiūros¹⁴.

2025 m. *Palantir* kapitalizacija (akcijų vertė rinkoje) pasiekė 400 mlrd. JAV dolerių¹⁵.

Pasibaigus 2026 m. pirmajam ketvirčiui skelbta, kad *Palantir Technologies* gavo 1,63 mlrd. JAV dolerių pajamų ir kad šis bendrovės rodiklis per metus išaugo 85 proc. Tai sparčiausias pajamų šuolis nuo *Palantir* debiuto biržoje 2020 m. Per metus kompanijos grynasis pelnas išaugo maždaug keturgubai – nuo 214 mln. iki 870,5 mln. JAV dolerių¹⁶.

Žurnalo *Forbes* 2025 metų rugsėjo duomenimis, du iš įmonės steigėjų – Peteris Thielis ir Alexas Karpas – yra tarp 100 turtingiausių amerikiečių¹⁷. 2026 m. gegužės 6 d. Thielio valdomo turto vertė siekė 28,3 mlrd. JAV dolerių¹⁸, Karpo – 13 mlrd. JAV dolerių¹⁹.

Pastaruoju metu abu šie asmenys patraukė visuomenės dėmesį politiniais ir ideologiniais pareiškimais. Antai uždary paskaitų ciklą rinkiniams klausytojams surengęs Thielis dėstė jiems apie Antikristą, kuris suvokiamas kaip kolektyvinė jėga, savotiška pasaulio valdžia, garantuojanti piliečiams saugumą, tačiau stabdanti inovacijas ir pažangą – taip pat ir DI plėtrą^{20, 21}.

Karpas sukėlė šurmulį 2026 m. balandžio 18 d. žinute socialiniame tinkle X paviešinęs vadinamąjį „*Palantir* manifestą“²². Dėl šio teksto Karpas sulaukė kritikos^{23, 24}.

„Manifestas“ yra trumpa Karpo knygos „Technologinė respublika“ (*The Technological Republic*) santrauka. Šią knygą jis parašė kartu su Nicholas'u Zamiska, atsakingu už *Palantir* korporatyvinius klausimus. 2025 m. išleista knyga, anot autorių, atspindi įmonės veiklos „teorinius“ pagrindus²⁵.

„Manifeste“ aptariamoms temoms driekiasi nuo būtinybės Silicio slėniui dalyvauti JAV gynybos reikaluose ir siūlymo įvesti privalomąją karinę tarnybą iki vienu kultūrų viršenybės prieš kitas.

Pvz., Karpo teigimu, dabar visos kultūros laikomos lygiomis, o kritika ir subjektyvūs vertinimai draudžiami. „Bet ši dogma ignoruoja tą faktą, kad tam tikros kultūros ir subkultūros darė stebuklus, tuo tarpu kitos buvo viso labo vidutinės ar dar blogiau – regresyvios ir kenksmingos“, – skelbiama 21-ajame manifesto punkte. Greta to kritikuojama kultūrinė įtrauktis ir pliuralizmas. Manifeste smerkiamas pokarinis Vokietijos ir Japonijos „nukenksminimas“. *Palantir* Vokietijos susilpninimą vadina „perdėta reakcija“, už kurią „Europa dabar moka didelę kainą“²⁶.

Dėl šio „manifesto“ Jungtinėje Karalystėje kai kurie politikai suabejojo valstybinių sutarčių su *Palantir* tikslingumu. *Palantir* yra sudariusi per 575 mln. eurų vertės sutarčių su šalies Vyriausybe, įskaitant 380

¹⁴ Montevirgen, K. (n. d.). Palantir Technologies, Inc. Prieiga per internetą: <https://www.britannica.com/money/Palantir-Technologies-Inc>

¹⁵ Palantir Is Now a \$400 Billion-Plus Company. (2025 m. rugsėjo 6 d.) Prieiga per internetą: <https://www.wsj.com/livecoverage/stock-market-today-dow-sp-500-nasdaq-08-06-2025/card/palantir-is-now-a-400-billion-plus-company-jKONqGtRU0BLhZyOMXx2>

¹⁶ Venckutė, A. (2026 m. gegužės 5 d.). „Palantir“ spartus šuolis – pajamos augo 85%. Prieiga per internetą:

<https://www.vz.lt/inovacijos/2026/05/05/palantir-spartus-suolis-pajamos-augo-85-584294>

¹⁷ The 400 Richest People In America (2025). Prieiga per internetą: <https://www.forbes.com/forbes-400/>

¹⁸ Peter Thiel. (2026 m. gegužės 6 d.). Prieiga per internetą: <https://www.forbes.com/profile/peter-thiel/>

¹⁹ Alexander Karp. (2026 m. gegužės 6 d.). Prieiga per internetą: <https://www.forbes.com/profile/alexander-karp/>

²⁰ Bullard, L. (2025 m. rugsėjo 30 d.). The Real Stakes, and Real Story, of Peter Thiel's Antichrist Obsession. Prieiga per internetą:

<https://www.wired.com/story/the-real-stakes-real-story-peter-thiels-antichrist-obsession/>

²¹ Bove, T. (2026 m. kovo 16 d.). Peter Thiel brings his Antichrist lectures to Rome – and Italian politicians are calling his ideas ‘scandalous’.

Prieiga per internetą: <https://fortune.com/2026/03/16/peter-thiel-antichrist-theory-rome-lectures-vatican-response/>

²² Because we get asked a lot. The Technological Republic, in brief. (2026 m. balandžio 18 d.). Prieiga per internetą:

<https://x.com/PalantirTech/status/2045574398573453312>

²³ Ehl, D. (2026 m. balandžio 23 d.). Palantir: Why its political manifesto is causing a stir. Prieiga per internetą:

<https://www.dw.com/en/palantir-why-its-political-manifesto-is-causing-a-stir/a-76895480>

²⁴ Down, A., Booth, R. (2026 m. balandžio 21 d.). Alarm caused by posts of Alex Karp, tech firm's CEO, championing US military dominance and of AI weapons. Prieiga per internetą: <https://www.theguardian.com/technology/2026/apr/21/palantir-manifesto-uk-contract-fears-mps>

²⁵ Einoris, T. (2026 m. balandžio 22 d.). „Palantir“ paskelbtas manifestas sukėlė audrą. Prieiga per internetą:

<https://www.delfi.lt/naujienos/uzsienyje/22-punktu-palantir-manifestas-sukele-audra-120240382>

²⁶ Ten pat.

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

mln. eurų vertės sutartį su jos Nacionaline sveikatos tarnyba²⁷. Gegužės 21 d. Londono meras Sadiqas Khanas užblokavo sostinės policijos sandorį su *Palantir* (perkamu paslaugų vertė – apie 50 mln. svarų sterlingų)²⁸.

Palantir „manifestas“ paskatino jau ne pirmus metus vykstančias diskusijas dėl vadinamosios Tamsiosios apšvietos, *technofašizmo* ir kitų ideologinių srovių, susijusių su technologijų (ypač DI) pažanga. Šių temų aspektai aptarti 2025 m. Lietuvos nacionalinės bibliotekos dviguboje analitinėje apžvalgoje ZD-2025-10 ir ZD-2025-11 „Demokratijos transformacija: kiekybiniai parametrai ir diskusijos dėl pamatinių sąvokų“²⁹. Apibendrintai galima teigti, kad dėl DI teisinio norminimo nėra visuotinio sutarimo, juolab skiriasi JAV ir Europos Sąjungos pozicijos³⁰.

3. *Palantir* ir kitos aukštųjų technologijų bendrovės Ukrainoje

DI kuriančios ir į ginkluotą integruojančios Vakarų bendrovės veikia Ukrainoje beveik nuo pat Rusijos agresijos prieš šią šalį pradžios (2022 m. vasario 24 d.)³¹. Amerikiečių žurnalas *TIME* 2024 m. vasario 26 d. išėjo su užrašu „Pirmasis DI karas“ (angl. *The First AI War*) ir Ukrainos žemėlapiu kontūru ant viršelio³².

Technologijų milžinės *Palantir*, *Microsoft*, *Amazon*, *Google*, *Starlink Services* dirba, kad apsaugotų Ukrainą nuo Rusijos kibernetinių atakų, perkeltų svarbius Vyriausybės duomenis į debesiją, taip pat palaikytų šalies ryšio sistemą³³. JAV veidų atpažinimo technologijų bendrovė *Clearview AI* suteikė savo įrangą daugiau nei 1,5 tūkst. Ukrainos pareigūnų, dirbančių 18 institucijų. Ji padėjo identifikuoti per 230 tūkst. rusų okupantų ir ukrainiečių kolaborantų, veikusių Ukrainos teritorijoje³⁴. Didelį tarptautinį rezonansą sukėlė Elono Musko valdomos bendrovės *Starlink Services* veikimas: 2026 metų vasario pradžioje buvo atjungti *Starlink* terminalai, kuriais naudojosi Rusijos kariuomenė³⁵.

Nemažai smulkesnių Amerikos ir Europos bendrovių, daugelis kurių plėtoja dronų technologijas, taip pat įkūrė padalinius Kijeve^{36, 37}. Pvz., tarp jų minimos kompanijos:

²⁷ Ten pat.

²⁸ Elgueta, A. (2026 m. gegužės 21 d.). Met Police Palantir contract blocked by City Hall. Prieiga per internetą:

<https://www.bbc.com/news/articles/clyp1e11px0o>

²⁹ Nacionalinė biblioteka, Informacijos analitikos skyrius (2025). Demokratijos transformacija: kiekybiniai parametrai ir diskusijos dėl pamatinių sąvokų (ZD-2025-10 ir ZD-2025-11). Prieiga per internetą: https://www.lnb.lt/media/public/documents/analitines-apzvalgos/ZD-2025-10_ir_ZD-2025-11.pdf

³⁰ Venckutė, A. (2025 m. balandžio 3 d.). JAV užsimojus švelninti DI reguliavimą, ES bijo tapti „inovacijų muziejumi“. Prieiga per internetą:

<https://www.vz.lt/technologijos/2025/04/03/jav-uzsimojus-svelninti-di-reguliuojama-es-bijo-tapti-inovaciju-muziejumi-565550>

³¹ Bergengruen, V. (2024 m. vasario 8 d.). How Tech Giants Turned Ukraine Into an AI War Lab. Prieiga per internetą:

<https://time.com/6691662/ai-ukraine-war-palantir/>

³² The *TIME* Magazine cover story "The First AI War" (2024 m. vasario 26 d.). Prieiga per internetą: <https://timecoverstore.com/featured/the-first-ai-war-time.html>

³³ Giles, K. (2023 m. rugsėjo 12 d.). Tech giants hold huge sway in matters of war, life and death. That should concern us all. Prieiga per internetą:

<https://www.theguardian.com/commentisfree/2023/sep/12/tech-giants-war-elon-musk-ukraine-starlink>

³⁴ Dave, P., Dastin, J. (2022 m. kovo 14 d.). Exclusive: Ukraine has started using Clearview AI's facial recognition during war. Prieiga per internetą:

<https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/>

³⁵ Adams, P. (2026 m. vasario 19 d.). Musk cuts Starlink access for Russian forces - giving Ukraine an edge at the front. Prieiga per internetą:

<https://www.bbc.com/news/articles/c0q3ndj7052o>

³⁶ How Ukraine Became a Global Reference Point for AI-Driven Warfare. (2026 m. sausio 2 d.). Prieiga per internetą:

<https://digitalstate.gov.ua/news/tech/shi-na-viyini-chomu-ukrayinsky-dosvid-vykhodyt-za-mezi-defens-i-zminiuye-model-tyfrovyi-derzavy>

³⁷ How Ukraine and U.S. tech firms build for the future. (2023 m. liepos 26 d.). Prieiga per internetą: <https://ge.usembassy.gov/how-ukraine-and-u-s-tech-firms-build-for-the-future/>

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

- **Primer AI** (JAV) taiko DI analizuoti priešo komunikavimą rusų kalba beveik realiuoju laiku³⁸;
- **Shield AI** (JAV) specializuojasi DI valdomų dronų srityje, kuria apsaugą nuo navigacijos trikdžių³⁹;
- **Scale AI** (JAV) realiuoju laiku analizuoja palydovines nuotraukas vertinant atakų žalą pastatams bei infrastruktūrai⁴⁰;
- **Helsing GmbH** (Vokietija) kuria DI sistemas dronams⁴¹.

2026 metų balandžio viduryje vykusio Ukrainos prezidento Volodymyro Zelenskio vizito Vokietijoje metu buvo pasirašytos kelios sutartys dėl ginkluotės vystymo su vokiečių kompanijomis, tarp kurių paminėtos *Quantum Systems*, *POINToX*, *Diehl*⁴².

Kalbant apie Ukrainoje dirbančias kompanijas, *Palantir Technologies* yra bene žinomiausia pasaulyje. Jos vadovas Karpas vyko į užpultąją šalį praėjus maždaug trimis mėnesiams nuo Rusijos agresijos pradžios – 2022 m. birželio 1 d.⁴³

Pasak Karpo, pasitelkiant *Palantir* programas nustatoma didelė dalis taikinių, kuriuos atakuoja Ukrainos kariuomenė, taigi bendrovės technologija tapo esminiu „skaitmeninio karo“ įrankiu. Įmonė teikia programas, kurios padeda kariuomenei realiu laiku apdoroti milžiniškus duomenų kiekius ir priimti taktinius sprendimus. *Palantir* sistemos sujungia duomenis iš palydovų, dronų, radarų ir žvalgybos šaltinių, todėl greitai identifikuojamos priešo pozicijos (tankai, artilerija), ir jų koordinatės perduodamos artilerijos padaliniais. *Palantir* įranga leidžia analizuoti mūšio lauko dinamiką, prognozuoti priešo veiksmus, efektyviau skirstyti amuniciją bei išteklius⁴⁴. Padedant *Palantir* Ukraina labai pagerino oro gynybos galimybes⁴⁵. Negana to, *Palantir* programos naudojamos išminavimo darbams⁴⁶, taip pat karinei logistikai optimizuoti⁴⁷.

Palantir kartu su Ukrainos gynybos ministerija sukūrė skaitmeninę platformą *Brave1 Dataroom*, skirtą DI modelių vystymui ir testavimui naudojant realius mūšio lauko duomenis. Ši iniciatyva leidžia Ukrainos gynybos įmonėms pagreitinti autonominių sistemų, ypač skirtų kovai su dronais, kūrimą⁴⁸. *Brave1* teikiamomis galimybėmis naudojami tokios Ukrainos kompanijos kaip *Osavul*, kovojanti su Rusijos

³⁸ Primer Senior Director of Data Science explores the future of AI in warfare. (n. d.). Prieiga per internetą: <https://primer.ai/news/primer-senior-director-of-data-science-explores-the-future-of-ai-in-warfare>

³⁹ Shield AI starts training with Ukraine's Unmanned Systems Forces, establishes local presence in Ukraine. (2025 m. sausio 16 d.). Prieiga per internetą: <https://shield.ai/shield-ai-starts-training-with-ukraines-unmanned-systems-forces-establishes-local-presence-in-ukraine/>

⁴⁰ Scale AI providing free datasets to help national security partners gain current insights into Russia-Ukraine conflict. (2022 m. kovo 7 d.). Prieiga per internetą: <https://scale.com/blog/ukraine-detection>

⁴¹ Helsing GmbH (n. d.). Prieiga per internetą: <https://www.reuters.com/company/helsing-gmbh/>

⁴² Strengthening Ukraine's Air Defense and Agreements on Drone Deals: Results of the President's Visits to Germany and Norway. (2026 m. balandžio 15 d.). Prieiga per internetą: <https://www.president.gov.ua/en/news/posilennya-ukrayinskoyi-ppo-ta-domovlenosti-pro-drone-deals-103885>

⁴³ Žr. 31 šaltinį.

⁴⁴ Ten pat.

⁴⁵ Tai keičia viską. Į Ukrainą žengia planas „Palantir“. Dangus bus uždarytas. (2026 m. sausio 23 d.). Prieiga per internetą:

<http://www.technologijos.lt/n/karyba/n/karyba/S-225425/straipsnis/Tai-keicia-viska-l-Ukraina-zengia-planas-Palantir-Dangus-bus-uzdarytas>

⁴⁶ Automation of demining processes and the use of AI: the Ministry of Economy signs a partnership agreement with Palantir. (2024 m. kovo 3 d.). Prieiga per internetą: <https://me.gov.ua/News/Detail?lang=en-GB&id=2e35612d-f83a-43af-bcd7-185b90c695c0&title=AutomationOfDeminingProcessesAndTheUseOfAi-TheMinistryOfEconomySignsAPartnershipAgreementWithPalantir>

⁴⁷ Kushnikov, V. (2023 m. gegužės 29 d.). Palantir Inc to provide IT assistance to the Ukrainian army. Prieiga per internetą: <https://military.com/en/news/palantir-inc-to-provide-it-assistance-to-the-ukrainian-army/>

⁴⁸ Ukraine Launches Brave1 Dataroom with Palantir to Train AI Models Using Battlefield Data. (2026 m. sausio 20 d.). Prieiga per internetą: <https://digitalstate.gov.ua/news/tech/ukraine-launches-brave1-dataroom-with-palantir-to-train-ai-models-using-battlefield-data>

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

dezinformacija⁴⁹, *Mantis Analytics*, taikanti DI informacinei erdvei stebėti realiuoju laiku, valdyti fizines ir informacines rizikas bei užtikrinti tiekimo grandinių saugumą⁵⁰.

Naudodamos *Palantir* sistemas *MetaConstellation* ir *Gotham*, Ukrainos pajėgos integruoja palydovinius vaizdus, radijo signalų perėmimus ir logistikos duomenis, ir tai leidžia identifikuoti Rusijos kariuomenės taikinius.

MetaConstellation veikia kosmose ir yra skirta valdyti bei optimizuoti palydovų tinklų duomenis realiu laiku. Sistema „orkestruoja“ kosminius palydovus. Dešimtys skirtingų komercinių ir valstybinių palydovų sujungiami į darniai veikiantį tinklą. Nereikia atskirai kreiptis į kiekvieną tiekėją, nes sistema pati parenka tinkamiausią palydovą užduočiai atlikti. Pvz., gavusi analitiko užklausą: „Kas pasikeitė šiame sektoriuje per pastarąsias 2 valandas?“, *MetaConstellation* automatiškai užsako vaizdus iš virš nurodytosios vietovės skrendančių palydovų, turinčių reikiamą jutiklį (pvz., „matantį“ per debesis). Kadangi duomenų siuntimas iš kosmoso į Žemę yra lėtas, dalis *Palantir* DI algoritmų veikia pačiuose palydovuose. Jie iškart atpažįsta taikinius (tankus, laivus) ir į Žemę siunčia ne milžiniškos apimties nuotraukas, o tik esminę informaciją⁵¹.

Taigi, integruodamos duomenis iš dronų, palydovų ir lauko jutiklių, *Palantir* ir kitos DI plėtojančios kompanijos kuria programas, pateikiančias išsamų mūšio lauko vaizdą. Tiek atskiri kovotojai, tiek ginklų sistemos tampa sudėtingų operacijų tinklų taškais. Informaciniame kare DI kuriančių bendrovių ištekliai padeda analizuoti socialinius tinklus ir kitus komunikacijos srautus, aptikti dezinformacijos kampanijas.

4. *Palantir* ir JAV valstybinės administracijos bendradarbiavimas

Palantir produktus šiuo metu naudoja tiek JAV ginkluotosios pajėgos, tiek civilinė administracija. ***Palantir* sistemos operacinė architektūra susideda iš trijų pagrindinių platformų: *Gotham*, *Foundry* ir *Apollo***⁵².

JAV Centrinės žvalgybos valdybos užsakymu sukurta platforma ***Gotham*** integruoja radijo žvalgybos, finansinių operacijų, palydovinių vaizdų, kompiuterijos skaitmenos duomenis ir kuria dinامينius rizikos žemėlapius.

Foundry išplečia *Palantir* galimybes veikti civilinėje srityje srityje. Kuriami kritinės infrastruktūros – energetikos tinklų, tiekimo grandinių, sveikatos priežiūros sistemų – skaitmeniniai „dvyniai“. *Foundry* leidžia imituoti įvairius raidos scenarijus ir numatyti krizes.

Apollo užtikrina *Palantir* sistemų atsparumą ir tęstinumą, įgalindama naujinimus realiuoju laiku ir jų diegimą net labai nepalankiomis aplinkybėmis. Būtent šis „orkestravimo“ sluoksnis leidžia *Palantir* veikti karo zonose esant kibernetinio ryšio sutrikimams.

⁴⁹ Müller, A. (2024 m. rugsėjo 14 d. (2024 m. rugsėjo 14 d.). Battling the echo chamber: Osavul's fight against Russian disinformation. Prieiga per internetą: <https://www.euronews.com/2024/09/15/battling-the-echo-chamber-osavuls-fight-against-russian-disinformation>

⁵⁰ Where supply chains simulate their next strategic decision. (n. d.). Prieiga per internetą: <https://mantisanalytics.com/>

⁵¹ MetaConstellation. (n. d.). Prieiga per internetą: <https://www.palantir.com/offerings/metaconstellation/>

⁵² Spagnuolo, G. (n. d.). Palantir and the Alchemy of Hybrid Power. Prieiga per internetą: <https://www.natofoundation.org/food/palantir-and-the-alchemy-of-hybrid-power/>

Trys platformos: *Gotham*, *Foundry*, *Apollo* kartu sudaro infrastruktūrą, kuria siekiama procesus paversti suprantamais, nuspėjamaiais ir todėl valdomais⁵³.

Tarp konkrečių *Palantir* programų taikymo pavyzdžių – **kovos su terorizmu atvejis**, t. y. bandymo surengti sprogdinimą Times aikštėje Niujorke organizatorių išaiškinimas (2010 m.)

2010 m. gegužės 1 d. nepavykus bandymui susprogdinti bombą Times aikštėje, Federalinis tyrimų biuras per *Gotham* sistemą operatyviai susiejo skirtingus duomenų taškus – finansines anomalijas, kelionių įrašus, komunikacijos metaduomenis – ir nustatė teroristą Faisalą Shahzadą. Ilgai netrukęs įtariamąjį identifikavimas ir suėmimas (per 53 val.) rodo *Palantir* programų gebėjimą spartinti tyrimo procesus⁵⁴. Tradiciniais metodais toks duomenų sujungimas būtų trukęs savaites, tačiau taikant *Palantir* programas įtariamąjį pavyko nustatyti labai greitai. Pareigūnai sulaukė Shahzadą lėktuve, kai šis jau ruošėsi kilti iš Niujorko skrydžiui į Dubajų⁵⁵.

Kita sėkmingo *Palantir* produktų panaudojimo sritis – **Europos energetikos infrastruktūros apsauga**. Pvz., po dujotiekio *Nord Stream* sprogdinimo 2022 m. rugsėjo 26 d.⁵⁶ Norvegija dislokavo *Foundry* povandeninius jutiklius stebėti jūrų eismą ir povandeninę struktūrą. 2022 metų spalį, *Foundry* aptikus anomalijų palei dujotiekį *Europipe II*, buvo surengta karinio jūrų laivyno operacija, kuri, tikėtina, užkirto kelią didelei diversijai, galėjusiai sukelti energijos tiekimo sutrikimus Europoje⁵⁷.

Palantir pasitarnauja ir **JAV bei NATO ginkluotosioms pajėgoms**. *Palantir* palaikoma ir plėtojama sistema *Project Maven* šiuo metu yra svarbiausia Pentagono DI programa. Ji startavo 2017 m. kaip siauro profilio eksperimentas, skirtas padėti karo analitikams susigaudyti iš konfliktų zonų plūstančioje dronų filmuotoje medžiagoje⁵⁸. Šį projektą iš pradžių plėtojo *Google*, bet dėl darbuotojų protestų prieš DI naudojimą karyboje iš jo pasitraukė. Nuo 2024 m. *Maven* perėmė *Palantir*.

2018 m. per 3 tūkst. *Google* darbuotojų pasirašė atvirą laišką, kuriuo išreiškė poziciją prieš bendrovės dalyvavimą šiame projekte. Keletas inžinierių netgi atsistatydino. Pasibaigus sutarties galiojimui, *Google* atsisakė ją pratęsti ir po to paskelbė DI principus, kuriuose aiškiai atmetama galimybė dalyvauti kuriant ginklų sistemas⁵⁹.

Palantir sukūrė ir išplėtojo *Maven Smart System*, kuri naudoja DI vaizdinės medžiagos iš dronų ir palydovų analizei bei padeda nustatyti taikinius bei vertinti grėsmes realiuoju laiku. 2026 metų kovą JAV Karo⁶⁰ departamentas nusprendė užtikrinant ilgalaikį *Maven* kaip pagrindinės kariuomenės sistemos

⁵³ Ten pat.

⁵⁴ Ten pat.

⁵⁵ Times Square bombing: trail that led to Faisal Shahzad. (2010 m. gegužės 5 d.). Prieiga per internetą:

<https://www.theguardian.com/world/2010/may/05/times-square-bombing-faisal-shahzad>

⁵⁶ Adomaitis, N., Ahlander J. (2025 m. rugpjūčio 22 d.). What is known about the Nord Stream gas pipeline explosions? Prieiga per internetą: <https://www.reuters.com/world/europe/what-is-known-about-nord-stream-gas-pipeline-explosions-2025-08-21/>

⁵⁷ Žr. 52 šaltinį.

⁵⁸ Lewis-Kraus, G. (2026 m. balandžio 16 d.). How Project Maven Put A.I. Into the Kill Chain. Prieiga per internetą:

<https://newyorker.substack.com/p/how-project-maven-put-ai-into-the>

⁵⁹ Dirbtinis intelektas kare: kas žinotina apie Pentagono programą „Project Maven“. (2026 m. balandžio 5 d.). Prieiga per internetą:

<https://www.lrt.lt/naujienos/mokslas-ir-it/11/2889024/dirbtinis-intelektas-kare-kas-zinotina-apie-pentagono-programa-project-maven>

⁶⁰ Trumpas pervadina JAV gynybos departamentą į „Karo departamentą“. (2025 m. rugsėjo 5 d.). Prieiga per internetą:

<https://www.lrt.lt/naujienos/pasaulyje/6/2666029/trumpas-pervadina-jav-gynybos-departamenta-i-karo-departamenta>

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

finansavimą⁶¹. *Palantir* platforma tapo ir transatlantiniu standartu – 2025 m. NATO oficialiai pradėjo naudoti *Maven Smart System* savo operacijoms⁶².

Project Maven sudaro svarbų JAV karinės operacijos prieš Iraną planavimo bei veiksmų elementą ir galimai yra tarp reikšmingiausių šiuolaikinio karo naujovių. Iki 2026 metų balandžio JAV ir Izraelio pajėgos, pasiremamos *Maven* duomenimis, atakavo maždaug 13 tūkst. taikinių⁶³.

Didelės konkurencijos sąlygomis kelios DI plėtojančios kompanijos ėmėsi valstybinės rangos kuriant naujos kartos karines sistemas. *Palantir* užsitikrino ilgalaikes pozicijas aptarnaujant JAV ginkluotąsias pajėgas. Valstybės priklausomybė nuo vieno stambaus tiekėjo sudaro prielaidas ir ideologinei įtakai, tokiai, kaip, pvz., išdėstyta kompanijos *Palantir* „manifeste“.

5. Kompanijos *Anthropic* etiniai principai

Šiame skyriuje nagrinėjamas konfliktas tarp amerikiečių kompanijos *Anthropic* ir JAV prezidento Donaldo Trumpo administracijos. *Anthropic* yra viena iš pirmaujančių DI sektoriaus įmonių – siekdama lyderystės technologijų srityje, ji skiria dešimtis milijardų JAV dolerių kompiuterinei infrastruktūrai⁶⁴.

Anthropic sukurtas didysis kalbos modelis *Claude* buvo naudojamas plėtoti ir įgalinti bendrauti natūralia kalba karinę sistemą *Maven*.

Didieji kalbos modeliai (angl. *Large Language Model*) yra DI sistemos, apmokytos naudojant milijonius tekstinių duomenų kiekius, kad gebėtų suprasti, apdoroti ir generuoti natūralią žmogaus kalbą⁶⁵.

Šiuo metu *Anthropic* ir Pentagono bendradarbiavimas sutrikęs dėl bendrovės reikalavimo nenaudoti *Claude* JAV piliečių sekimo tikslais, taip pat visiškai automatizuotiems smūgiams, kai kovos veiksmai vyksta be žmogaus įsikišimo.

2026 metų vasarį pasirodė pranešimų, kad Venesuelos prezidento Nicolás'o Maduro suėmimo operacijoje galimai pasitelktas *Claude*. Kariuomenės protokolai išties rodė, kad minėtas įrankis naudotas kaip *Maven Smart System* dalis. Tai buvo netikėta įrankį sukūrusiai bendrovei. Teigiama, kad *Anthropic* vadovas susisiekė su *Palantir*, kad išsiaiškintų, kaip konkrečiai *Claude* panaudotas Venesueloje. Kai ši užklausa galiausiai pasiekė Trumpo administraciją, buvo nuspręsta, kad *Anthropic*, kuri tuo metu derėjosi dėl sutarties su federaline Vyriausybe atnaujinimo, galbūt yra nepatikima partnerė. Netrukus *Anthropic*, nuogaustaudama dėl jos produktų taikymo masiniam vidaus sekimui ir be žmogaus įsikišimo veikiantiems autonominiams ginklams, atsisakė leisti Pentagonui juos naudoti. Šis ginčas baigėsi tuo, kad karo sekretorius Pete'as Hegsethas žinutėje socialiniame tinkle pavadino *Anthropic* riziką tiekimo grandinėms keliančia įmone – nuolatine grėsme nacionaliniam saugumui⁶⁶.

⁶¹ Jeans, D. (2026 m. kovo 21 d.). Exclusive: Pentagon to adopt Palantir AI as core US military system, memo says: Prieiga per internetą: <https://www.reuters.com/technology/pentagon-adopt-palantir-ai-as-core-us-military-system-memo-says-2026-03-20>

⁶² Maven Smart System: Innovating for the Alliance. (2026 m. kovo 5 d.). Prieiga per internetą: <https://blog.palantir.com/maven-smart-system-innovating-for-the-alliance-5ebc31709eea>

⁶³ The AI War on Iran: Project Maven, a Secretive Palantir-Run System, Helps Pentagon Pick Bomb Targets. (2026 m. kovo 31 d.). Prieiga per internetą: https://www.democracynow.org/2026/3/31/project_maven_manson_bloomberg_ai_warfare

⁶⁴ AI research and products that put safety at the frontier. (n. d.). Prieiga per internetą: <https://www.anthropic.com/>

⁶⁵ What are Large Language Models (LLMs)? (n. d.). Prieiga per internetą: <https://www.solix.com/kb/large-language-models/>

⁶⁶ Žr. 58 šaltinį.

Prezidentas Trumpas socialiniame tinkle *TRUTH Social* parašė: „JUNGTINĖS AMERIKOS VALSTIJOS NIEKADA NELEIS RADIKALIAI KAIRIAJAI, „WOKE“⁶⁷ KOMPANIJAI DIKTUOTI, KAIP MŪSŲ DIDŽIOJI KARIUOMENĖ TURĖTŲ KOVOTI IR LAIMĖTI KARUS! Šis sprendimas priklauso JŪSŲ VYRIAUSIAJAM VADUI ir nuostabiems lyderiams, kuriuos aš skiriu vadovauti mūsų kariuomenei.

Kairuoliai mulkiai iš *Anthropic* padarė KATASTROFIŠKĄ KLAIDĄ, bandydami GAŠDINTI Karo departamentą ir priversti jį paklusti savo paslaugų teikimo sąlygoms, o ne mūsų Konstitucijai. Jų savanaudiškumas kelia pavojų AMERIKIEČIŲ GYVYBĖMS, mūsų kariams ir mūsų nacionaliniam saugumui.

Todėl nurodau VISOMS Jungtinių Valstijų Vyriausybės federalinėms agentūroms TUOJ PAT NUTRAUKTI bet kokį *Anthropic* technologijų naudojimą⁶⁸.

Kitą dieną po šio įrašo, 2026 m. vasario 28 d., JAV pradėjo karinę operaciją prieš Iraną, kurios metu *Claude* buvo panaudotas⁶⁹.

Pentagonas gegužės pradžioje paskelbė apie susitarimus su septyniomis pirmaujančiomis DI bendrovėmis *SpaceX*, *OpenAI*, *Google*, *Nvidia*, *Reflection*, *Microsoft* ir *Amazon Web Services* dėl jų technologijų diegimo įslaptintuose kariniuose tinkluose. *Anthropic* buvo atmesta. Įrankis *Claude* buvo vienintelis, kurį leista pasitelkti įslaptintose JAV kariuomenės operacijose, ir, pasak šaltinių, jis tebėra naudojamas⁷⁰.

Baltųjų rūmų pareigūnai ėmėsi rengti instrukciją, kaip taikyti *Anthropic* produktus, atsižvelgiant į tai, kad kompanija pripažinta rizika tiekimo grandinėms⁷¹. 2026 metų balandžio vidurio duomenimis, nepaisant *Anthropic* ginčo su JAV valstybine administracija, kompanijos produktą *Mythos* naudojo Nacionalinė saugumo agentūra (angl. *National Security Agency*)⁷², derėtasi dėl galimybės naudoti DI modelį *Mythos* ir kitose JAV žinybose⁷³.

Pentagonas plečia DI rangovų ratą: minėtos septynios bendrovės bus integruotos į pažeidžiamiausias JAV karinių žinybų įslaptintas sistemas, kurios naudojamos planuoti misijas, nutaikyti ginklus ir kitiems tikslams⁷⁴.

⁶⁷ Lapinskas, M. (2023 m. gruodžio 1 d.). „Woke“ kultūra – progresyvumo iliuzija. Prieiga per internetą: <https://www.bernardinai.lt/woke-kultura-progresyvumo-iliuzija/>

⁶⁸ Trump, D. (2026 m. vasario 27 d.). THE UNITED STATES OF AMERICA WILL NEVER ALLOW A RADICAL LEFT... Prieiga per internetą: <https://truthsocial.com/@realDonaldTrump/posts/116144552969293195>

⁶⁹ Žr. 59 šaltinį.

⁷⁰ Pentagonas pasirašė įslaptintus susitarimus su pirmaujančiomis DI įmonėmis, bet atmetė „Anthropic“. (2026 m. gegužės 1 d.). Prieiga per internetą: <https://www.vz.lt/inovacijos/2026/05/01/pentagonas-pasirase-islaptintus-susitarimus-su-pirmaujančiomis-di-imonėmis-bet-atmete-anthropic-584203>

⁷¹ Curi, M. Gold, A. (2026 m. balandžio 28 d.). Scoop: White House workshops plan to bring back Anthropic. Prieiga per internetą: <https://www.axios.com/2026/04/29/trump-anthropic-pentagon-ai-executive-order-gov>

⁷² Ten pat.

⁷³ Ten pat.

⁷⁴ Ten pat.

Jungtinių Valstijų pavyzdys rodo, kad itin sparti karinio DI plėtra baigiasi situacijomis, kai DI sistemos tampa kritinėmis – ypač ginčo tarp jas kuriančių kompanijų ir valstybės atveju. Tai verčia valstybę skubiai ieškoti pakaitalų, kartu keliant pavojų karinio planavimo lygiui ir operacijų kokybei.

6. DI taikymas Izraelio karinėse operacijose Vakarų Krante ir Palestinoje

Šiame skyriuje nagrinėjami keliu Izraelio kariuomenės sistemų, veikiančių DI pagrindu, naudojimo etiniai ir teisiniai aspektai.

2023 metų lapkritį leidiniai *+972 Magazine* ir *Local Call* paskelbė bendrą ataskaitą apie Izraelio gynybos pajėgų (angl. *Israel Defense Forces*, IDF) vykdytas operacijas⁷⁵. Ataskaitos duomenimis, IDF naudojo sistemas *Lavender* ir *Gospel*, į kurias integruotas DI. Tyrėjai teigė, kad sistemos, be kita ko, automatiškai teikia rekomendacijas, kur ir kaip pulti privačius namus, kuriuose gyvena asmenys, galimai priklausantys „Hamas“ arba „Islamo džihadui“ (abi šios organizacijos pripažintos teroristinėmis ir ES, joms taikomos sankcijos⁷⁶). Šią temą išplėtojo pasaulyje plačiai skaitomas britų leidinys *The Guardian*⁷⁷, ir tai sukėlė tarptautines diskusijas dėl IDF veiksmų teisėtumo⁷⁸.

Gospel yra sistema, sujungianti įvairius informacijos sluoksnius potencialiems kariniams taikiniams nustatyti, o *Lavender* yra išmanioji duomenų bazė, siejanti ir rūšiuojanti informaciją apie galimus „Hamas“ ar kitų organizuotų ginkluotų grupuočių narius. *Lavender* duomenų bazė didelė, pvz., po 2023 m. spalio 7 d. teroristinio išpuolio⁷⁹ prasidėjus naujausiems karo veiksams su Izraeliu „Hamas“ turėjo iki 40 tūkst. narių. „Islamo džihadas“ turi kelis tūkstančius kovotojų⁸⁰.

Remiantis *+972 Magazine* ataskaita, *Lavender* įtaka kariuomenės operacijoms buvo tokia, kad kariškiai iš esmės traktavo DI pateiktus rezultatus, tarsi tai būtų žmogaus sprendimai⁸¹. Ataskaitoje rašoma, kad kariuomenė leido karininkams priimti „žudymo sąrašus“ nereikaludama nuodugniai patikrinti, kodėl *Lavender* pateikė tokius sprendimus. Pranešama, kad kariškiai kartais patvirtindavo nuosprendžius per 20 sekundžių⁸².

⁷⁵ Dixon, L. (2025 m. gegužės 26 d.). *+972 and Local Call: Investigating Israel at War*. Prieiga per internetą: <https://gijn.org/stories/investigating-israel-war-972-local-call/>

⁷⁶ „Hamas“ ir Palestinos islamo džihadas: Taryba pratęsė ribojamųjų priemonių galiojimą dar vieniems metams. (2026 m. sausio 16 d.). Prieiga per internetą: <https://www.consilium.europa.eu/lt/press/press-releases/2026/01/16/hamas-and-palestinian-islamic-jihad-council-prolongs-restrictive-measures-for-another-year/>

⁷⁷ Viner, K. (n. d.). Since 1821 the mission of the Guardian has been to use clarity and imagination to build hope. Prieiga per internetą: <https://www.theguardian.com/about>

⁷⁸ McKernan, B., Davies H. (2024 m. balandžio 3 d.). 'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets. Prieiga per internetą: <https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes>

⁷⁹ „Hamas“ Spalio 7-osios ataką vadina istoriniu atsaku į Izraelio veiksmus. (2025 m. spalio 10 d.). Prieiga per internetą:

<https://www.15min.lt/naujiena/aktualu/pasaulis/hamas-spalio-7-osios-ataka-vadina-istoriniu-atsaku-i-izraelio-veiksnius-57-2539202>

⁸⁰ Schmitt, M. (2024 m. birželio 28 d.). Israel - Hamas 2024 Symposium - The Gospel, Lavender, and the Law of Armed Conflict. Prieiga per internetą: <https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/>

⁸¹ Ten pat.

⁸² Ten pat.

IDF atstovai tokius žiniasklaidos teiginius atmetė – esą, „visais atvejais būtinas atskiras [žvalgybos] analitiko tyrimas, patvirtinantis, kad nustatytieji taikiniai yra teisėti pagal IDF direktyvas ir tarptautinėje teisėje nustatytas sąlygas“⁸³. Pasak IDF, įrankis *Gospel* nenaudojamas gyviesiems taikiniams nustatyti. Jis informuoja žvalgybos analitikus apie objektus (pvz., pastatus ir kitokią infrastruktūrą), kurie gali būti laikomi kariniais taikiniais, ir vadovaujasi ginkluoto konflikto teise (angl. *Law of Armed Conflict, LOAC*)⁸⁴. Kariuomenės analitikai privalo įvertinti duomenis, remdamiesi standartine veiklos procedūra (*Standard Operating Procedure*)⁸⁵, kuri taiko kariniams objektams kriterijus, nustatytus 1977 m. 1-ojo papildomo protokolo prie 1949 m. Ženevos konvencijų 52(2) straipsnio. Izraelis nėra 1-ojo papildomo protokolo šalis, tačiau, kaip ir Jungtinės Valstijos, pripažįsta šią nuostatą kaip tikslią tarptautinės teisės formuluotę. Pagrindiniai 52(2) straipsnio principai:

- civiliniai objektai, kurie nėra kariniai taikiniai (gyvenamieji namai, mokyklos, maldos namai ir kt.), negali būti atakuojami.
- Jei kyla abejonų, ar civiliniams reikalams skirtas objektas (pvz., bažnyčia, mokykla) yra naudojamas karinei veiklai, laikoma, kad jis nėra naudojamas kariniais tikslais (nekarinio naudojimo prezumpcija).
- Infrastruktūra, tokia kaip tiltai, elektrinės ar komunikacijų centrai, dažnai laikoma dvejopos paskirties objektais. Jie tampa teisėtu taikiniu tik tada, kai reikšmingai papildo prieš karinius pajėgumus^{86, 87}.

Taisyklės, reglamentuojančios taikinių nustatymą^{88, 89}, teoriškai yra gana paprastos, nors jų taikymas mūšio lauke gali būti sudėtingas. Teisėtiems taikiniams nustatyti taikomi trys punktai⁹⁰:

- puolami gali būti tik kariniai taikiniai, kovotojai, organizuotų ginkluotų grupuočių nariai ir tiesioginiai karo veiksmų dalyviai.
- Puolantysis privalo imtis visų įmanomų atsargumo priemonių, kad kuo labiau sumažintų žalą civiliniams objektams ir išvengtų civilių žalojimo ar mirties (vadinamosios šalutinės žalos).
- Tikėtina šalutinė žala negali būti per didelė, palyginti su numatoma konkrečia ir tiesiogine karine nauda (proporcingumo principas).

IDF teigimu, *Gospel* ir *Lavender* naudojimas pagrįstas pirmosios taisyklės taikymu. Jei DI sistema pasitelkiama laikantis pagrįstų procedūrų, ji turėtų pagerinti puolančiosios pajėgos gebėjimą patikimai identifikuoti teisėtus taikinius: objektus ir asmenis.

⁸³ Ten pat.

⁸⁴ Introduction to the Law of Armed Conflict (LOAC). (2023 m.). Prieiga per internetą: <https://www.genevacall.org/wp-content/uploads/2023/07/The-Law-of-Armed-Conflict.pdf>

⁸⁵ Standard Operating Procedure. (2025 m.). Prieiga per internetą: [https://resourcehub01.blob.core.windows.net/\\$web/Policy%20and%20Guidance/corepeacekeepingguidance/Thematic%20Operational%20Activities/Military/2025.17%20Standard%20Operating%20Procedure%20on%20Selection%20of%20Military%20Units%20\(SOP\).pdf](https://resourcehub01.blob.core.windows.net/$web/Policy%20and%20Guidance/corepeacekeepingguidance/Thematic%20Operational%20Activities/Military/2025.17%20Standard%20Operating%20Procedure%20on%20Selection%20of%20Military%20Units%20(SOP).pdf)

⁸⁶ Ženevos konvencijos (dėl karo aukų). (2025 m. rugsėjo 8 d.). Prieiga per internetą: <https://www.urm.lt/tarptautines-sutartys/konvencijos/zenevos-konvencijos-del-karo-auku/673>

⁸⁷ Article 52 - General protection of civilian objects. (n. d.). Prieiga per internetą: <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52>

⁸⁸ Žr. 84 šaltinį.

⁸⁹ General Background and Basic Principles of the Law of Armed Conflict. (n. d.). Prieiga per internetą: <https://biotech.law.lsu.edu/blog/Basics-of-Law-of-Armed-Conflict.pdf>

⁹⁰ Targeting under International Humanitarian Law. (n. d.). Prieiga per internetą: <https://casebook.icrc.org/highlight/targeting-under-international-humanitarian-law>

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

Apibendrinant galima teigti, kad DI sistemų taikymas karyboje priklauso nuo jas naudojančios pusės požiūrio į karinę teisę ir karybos taisykles. Laisvoji žiniasklaida, veikianti demokratijos sąlygomis, įgalina teisės pažeidimų fiksavimą ir didesnę ar mažesnę kariuomenės kontrolę.

7. Microsoft ir Izraelio žvalgybos bendradarbiavimo užkulisiai

Šiame skyriuje nušviečiamos aplinkybės, kuriomis kompanija *Microsoft* nutraukė bendradarbiavimą su Izraelio žvalgyba.

Microsoft debesijos platforma *Azure* buvo plačiai naudojama Izraelio karinės žvalgybos, ypač vadinamojo 8200-ojo padalinio operacijose⁹¹. Partnerystė, slapta pradėta 2021 m., įgavo precedento neturintį mastą, kadangi *Microsoft* teikė ne tik debesijos infrastruktūrą, bet ir personalą, patirtį bei žvalgybai pritaikytą DI⁹². 8200-asis padalinys naudojo naują sistemą, leidžiančią jo žvalgybos pareigūnams rinkti, atkurti ir analizuoti visos palestiniečių populiacijos mobiliųjų skambučių turinį vieno mln. skambučių per valandą apimtimi. *Azure* infrastruktūra tapo viena pažangiausių pasaulyje stebėjimo sistemų⁹³.

2025 m. viduryje *Microsoft* serveriuose buvo saugoma beveik 11 500 terabaitų karinių duomenų, kuriais naudojosi Izraelio žvalgyba – tai atitinka per 200 milijonų valandų pokalbių įrašų. Duomenys apėmė perimtą komunikaciją, įskaitant maždaug 1 mln. palestiniečių telefoninių skambučių per valandą. Ši masinė duomenų rinkimo ir analizės operacija, sustiprinta DI įrankių, tokių kaip kalbos atpažinimo ir dokumentų santraukų rengimo priemonės, buvo labai svarbi planuojant oro antskrydžius, vykdant areštus ir nustatant taikinius Gazos Ruože bei Vakarų Krante⁹⁴.

Microsoft tvirtino, kad jos technologijos pirmiausia pasitelkiamos gynybos tikslais ir kibernetinei apsaugai. Tačiau buvę ir esami darbuotojai bei atskleisti vidiniai dokumentai piešia kitokį vaizdą. Suteiktos priemonės ir aplinka buvo tiesiogiai naudojamos puolamosiose operacijose, kurių poveikis buvo įvairus – nuo tikslinių nužudymų iki masinių sulaikymų⁹⁵.

Reaguodama į *The Guardian* publikuotą medžiagą⁹⁶, bendrovė *Microsoft* nurodė skubiai atlikti vidinį tyrimą. Jo išvados paskatino bendrovę atšaukti 8200-ojo padalinio prieigą prie kai kurių debesijos saugyklų ir DI intelekto paslaugų⁹⁷.

⁹¹ Grigione, E. (2025 m. rugpjūčio 10 d.). Cloud, Codes and Conflict: How Microsoft Azure Became the Backbone of Unit 8200's Intelligence Architecture. Prieiga per internetą: <https://www.linkedin.com/pulse/cloud-codes-conflict-how-microsoft-azure-became-unit-8200s-grigione-dm7ef>

⁹² Davies, H., Abraham, Y. (2025 m. rugpjūčio 6 d.). 'A million calls an hour': Israel relying on Microsoft cloud for expansive surveillance of Palestinians. Prieiga per internetą: <https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud>

⁹³ Žr. 91 šaltinį.

⁹⁴ Ten pat.

⁹⁵ Ten pat.

⁹⁶ Žr. 92 šaltinį.

⁹⁷ Žr. 91 šaltinį.

Bendrovės sprendimas buvo priimtas atsižvelgiant į darbuotojų ir investuotojų spaudimą dėl jos darbo Izraelio kariuomenei ir *Microsoft* technologijų vaidmens vykstant karui Gazoje.

Kaip matyti, šiuo atveju DI taikymo teisėtumu suabejojo *Microsoft* darbuotojai ir akcininkai, paskatinti žiniasklaidoje paskelbtos medžiagos. Šis pavyzdys dar kartą patvirtina, kad informacijos apie abejotinę DI naudojimą pateikimas į viešąją erdvę gali sužadinti įvairių visuomenės grupių atsaką.

8. Apibendrinimas ir akcentai, į ką atkreipti dėmesį ateityje

Šiuo metu DI vystymo srityje vienaip ar kitaip konkuruoja visos technologijų gigantės, vadinamosios *Big Tech* bendrovės. Daugelis jų siekia valstybinių užsakymų. Itin sparti karinio DI plėtra lemia situacijas, kai DI sistemos tampa kritinėmis – ypač ginčų tarp kompanijų ir valstybės atveju. Tai verčia valstybę skubiai ieškoti pakaitalų, kartu keliant pavojų karinio planavimo lygiui ir operacijų kokybei.

Integruodamos dronų, palydovų ir lauko jutiklių duomenis, *Palantir* ir kitos DI plėtojančių kompanijų programos pateikia išsamų mūšio lauko vaizdą. Tiek atskiri kovotojai, tiek ginklų sistemos tampa sudėtingų operacijų tinklų taškais. Informaciniame kare DI bendrovių išteklių padeda analizuoti socialinius tinklus ir kitus komunikacijos srautus, aptikti dezinformacijos kampanijas.

Kompanija *Palantir*, veikianti ir Lietuvoje, yra viena didžiausių JAV valstybinės administracijos partnerių, be to, pasižymi savitomis ideologinėmis nuostatomis. „Palantir manifestas“ paaštrino jau ne pirmus metus vykstančias diskusijas dėl vadinamosios Tamsiosios apšvietos, *technofašizmo* ir kitų ideologinių srovių, susijusių su technologijų (ypač DI) pažanga. Dėl DI teisinio norminimo nėra visuotinio sutarimo, juolab skiriasi JAV ir ES pozicijos.

DI sistemų taikymas karyboje priklauso nuo jas taikančios pusės požiūrio į karo teisę ir karybos taisykles. Laisvoji žiniasklaida, veikianti demokratijos sąlygomis, įgalina teisės pažeidimų fiksavimą ir didesnę ar mažesnę kariuomenės kontrolę. Informacijos apie klausimų keliantį DI naudojimą nutekėjimas į viešąją erdvę gali sužadinti įvairių visuomenės grupių atsaką.

Akcentai, į ką atkreipti dėmesį ateityje

- Atsakingos Lietuvos institucijos turėtų nuolatos stebėti DI plėtros tendencijas ir vertinti, kaip šalies ginklavimosi programos galėtų paveikti DI taikymas karyboje.
- Nors užsienio kompanijos, bendradarbiaujančios su Lietuva duomenų apdorojimo srityje, garantuoja jų saugumą, šalies valstybinė administracija privalo nuolatos vertinti, kiek toks bendradarbiavimas atitinka Lietuvos nacionalinius interesus.