Dirbtinio intelekto technologijos ir jų taikymas gynyboje

Valdas Kriauza
Generolo Jono Žemaičio Lietuvos karo akademijos
Bibliotekos duomenų bazių administratorius

Pasaulio ekonomikos forumo įkūrėjas Klausas Schwabas mūsų gyvenamą laikotarpį pavadino Ketvirtąja pramonės revoliucija. Ši revoliucija, paremta ankstesniais išradimais, pasitelkusi skaitmeniniame amžiuje sukurtas technologijas, sukėlė didžiulį inovacijų šuolį – buvo pristatytos tokios technologijos, kaip papildytoji realybė ir daiktų internetas, robotika ir autonominės sistemos bei dirbtinis intelektas (toliau – DI) [1]. Jau šiandien DI sprendimai daro reikšmingą teigiamą poveikį ekonomikai, skatindami įmonių konkurencingumą ir didindami viešojo sektoriaus veiklos efektyvumą. DI technologijos, naudojamos tiek privačiame, tiek viešajame sektoriuose, sėkmingai pritaikomos ir saugumo bei gynybos srityse. Jos turi didžiulį potencialą sustiprinti gynybinius pajėgumus, sumažinti žmonių vaidmenį kare ir yra itin svarbios mažesnėms valstybėms, kurios privalo veikti turėdamos ribotus resursus.

Dirbtinio intelekto atsiradimas ir evoliucija

Terminas „dirbtinis intelektas“ pirmą kartą pavartotas 1956 m., kai Dartmuto koledže susibūrė įvairių sričių mokslininkų grupė, siekdama sukurti mokslo sritį, orientuotą į mašinų, gebančių imituoti žmogaus intelektą, kūrimą. Per porą dešimtmečių DI srityje įvyko reikšmingų proveržių. 1966 m. buvo sukurtas pirmasis kalbos apdorojimo įrankis „Eliza“, sugebantis palaikyti paprastą po-

kalbį su žmogumi. Kitas svarbus ankstyvojo DI laikotarpio projektas buvo GPS (angl. *General Problem Solver*) programa, kuri automatiškai gebėjo spręsti nesudėtingus matematikos uždavinius. Šie pasiekimai paskatino didžiules investicijas į DI tyrimus ir net buvo manoma, kad artimiausiu metu bus sukurta mašina, intelektu prilygstanti vidutiniam žmogui. Tačiau šie lūkesčiai nepasiteisino dėl ankstyvųjų DI sistemų ribotumo – jos žmogaus intelektą bandė imituoti remdamosi griežtomis taisyklėmis ir nebuvo pakankamai lanksčios įveikdamos sudėtingesnes užduotis. Dar XX a. 5-ojo dešimtmečio pabaigoje buvo pradėti neuronų tinklų tyrimai, kurių tikslas buvo sukurti DI, kuris veiktų imituodamas procesus, vykstančius žmogaus smegenyse. Tačiau šis darbas sustojo paaiškėjus, kad kompiuteriams trūksta skaičiuojamosios galios dirbti su tokiais neuronų tinklais [2]. Dirbtiniai neuronų tinklai sugrįžo giliojo mokymosi (angl. *Deep Learning*) pavidalu, o tikrasis jų proveržis įvyko XXI a. 1-ojo dešimtmečio viduryje. Šiandien dauguma programų, priskiriamų DI, yra pagrįstos dirbtiniais neuronų tinklais ir giliuoju mokymusi. Būtent šios technologijos sudaro vaizdų ir garso atpažinimo algoritmų pagrindą.

Dirbtinis intelektas saugumo ir gynybos sektoriuje

Naujos technologijos ir karyba visada buvo glaudžiai susijusios. Inovacijos mūšio lauke ne tik keitė karo pobūdį, bet ir suteikė strateginį bei taktinį pranašumą. DI nėra išimtis. Jo potencialas saugumo ir gynybos srityse buvo pastebėtas gana anksti. Daugelis karinių sistemų buvo automatizuojamos, nors dažnai tai nebuvo siejama su DI. Jau XX a. 5-ajame dešimtmetyje pradėta oro gynybos radarus aprūpinti siųstuvais-imtuvais, kurie padėdavo operatoriams, o vėliau ir patys galėjo nustatyti, ar stebimas lėktuvas yra draugiškas ar priešiškas. Vėliau buvo sukurtos taktinės ir strateginės įspėjimo sistemos, gebančios atskirti lėktuvus ir paleistas raketas pagal jų greitį, formą ar šilumos pėdsaką, lygindamos radarų duomenis su duomenų bazėje esančiomis grėsmėmis. XX a. 8-ajame dešimtmetyje raketos „oras–žemė“ ir „oras–oras“ jau galėjo automatiškai

koreguoti kursą arba rasti taikinį naudodamos radarus ar į šilumą reaguojančius taikiklius. Per kitus porą dešimtmečių oro gynybos sistemos tapo dar sudėtingesnės – jos jau galėjo pasiūlyti taikinių pasirinkimo galimybes ar net savarankiškai atakuoti taikinius automatiniu režimu [3].

Vis dėlto reikšmingiausias proveržis DI tyrimuose įvyko praėjusio amžiaus pabaigoje, iš esmės pasikeitus požiūriui į DI kūrimą. Jei anksčiau tyrimai daugiausia buvo grindžiami programavimu ir sudėtingais skaičiavimais, tai šiuolaikiniai metodai koncentruojasi į mašinų mokymąsi. Per pastaruosius porą dešimtmečių DI tyrimai padarė didžiulę pažangą tokiose srityse, kaip kompiuterinė rega, kalbos atpažinimas, natūralios kalbos apdorojimas ir robotika. Šios technologijos jau dabar sėkmingai pritaikomos saugumo ir gynybos srityse. Nors daugiausia diskusijų sulaukia su autonominėmis ginklų sistemomis susiję etikos klausimai, DI pritaikymo gynybos sektoriuje galimybės yra gerokai platesnės. DI gali būti taikomas žvalgyboje ir stebėjimo veiksmuose, logistikoje, kibernetinės saugos srityje, mūšio lauko valdymo ir sprendimų priėmimo procesuose, informacinėse operacijose, pusiau autonominėse arba autonominėse transporto priemonėse, povandeninių minų aptikimo ir kitose srityse.

Žvalgyba ir stebėjimas

Žvalgyba ir stebėjimas yra viena iš sričių, kurioje karinės pramonės investicijos į DI vienos didžiausių, ir tikėtina, kad ši tendencija tęsis. Bepiločių orlaivių naudojimas žvalgybai ir kibernetinės erdvės stebėjimas generuoja milžinišką kiekį duomenų. Šių duomenų apdorojimą itin palengvina mašinos, naudojančios DI. Vienas iš JAV gynybos departamento vykdomo projekto „Maven“ tikslų – integruoti kompiuterinės regos ir DI algoritmus, kurie analizuotų žvalgybos medžiagą ir automatiškai identifikuotų priešišką veiklą ir taikinius. DI automatizuotų veiklą analitikų, kurie praleidžia daugybę valandų peržiūrėdami bepiločių orlaivių surinktą medžiagą, užuot tą laiką skyrę veiksmingesniems laiku priimamiems

sprendimams. JAV žvalgybos ir pažangiųjų tyrimų agentūros vykdo projektus, kuriuose DI bus taikomas vaizdams atpažinti ir prognozuojamajai analizei. Kuriami daugiakalbio kalbos atpažinimo ir vertimo triukšmingoje aplinkoje, vaizdų be metaduomenų geolokacijos nustatymo, dvimačių vaizdų sujungimo į trimačius modelius algoritmai bei algoritmai įrankiams, leidžiantiems nustatyti pastatų paskirtį remiantis stebėjimo duomenimis [3].

Nors DI gali palengvinti žvalgybos analitikų darbą apdorodamas didelius kiekius duomenų, jo taikymas susiduria su rimtais iššūkiais dėl griežtų tikslumo ir saugumo reikalavimų. Pagrindinės problemos apima algoritmų nepatikimumą, didžiųjų duomenų analizės neapibrėžtumą ir saugumo rizikas debesijos technologijose. Be to, sėkmingam DI integravimui būtini įvairūs aukštos kokybės duomenys, suderinamumas su esamomis sistemomis, taip pat etinių, socialinių, privatumo ir saugumo aspektų įvertinimas, nes DI naudojimas žvalgyboje apima jautrios informacijos rinkimą ir analizę [4].

Planavimas ir logistika

DI turi milžinišką potencialą planavimo ir logistikos srityse. Vienas iš pirmųjų sėkmingų DI naudojimo pavyzdžių yra Dinaminės analizės ir perplanavimo įrankis (toliau – DART), kuris padėjo perkelti karius ir įrangą iš Europos į Saudo Arabiją dėl operacijų „Dykumos skydas“ ir „Dykumos audra“. Tai buvo didžiausia, tolimiausia ir greičiausiai įvykdyta logistinė operacija karo istorijoje, surengta vietovėje, kurioje anksčiau nebuvo dislokuota nei karių, nei atsargų. Pasak tuomečio JAV pažangiųjų gynybos projektų agentūros (angl. *Defense Advanced Research Projects Agency* – DARPA) direktoriaus Victoro Reiso, DI pagrįsta sprendimų paramos programa per kelis mėnesius atpirko visas DARPA tris dešimtmečius trukusias investicijas į DI technologijas [5].

Predikcinė analizė – dar viena sritis, kurioje sėkmingai taikomas DI. Ši technologija jau dabar naudojama ne tik komercinėse oro linijose, bet ir JAV karinių oro pajėgų lėktuvuose. Įprastai

techninė priežiūra vykdoma tik sugedus orlaiviui arba laikantis numatytų techninės priežiūros tvarkaraščių. Naudodamasis informacija, gauta iš varikliuose ir kitose sistemose sumontuotų daviklių, ir pasitelkdamas prognozuojamuosius algoritmus, DI padeda technikams pastebėti ankstyvus gedimų požymius ir įvertinti, kada orlaiviams reikalinga techninė priežiūra ar remontas [6]. IBM sukurta DI sistema „Watson“, analizuodama informaciją, surinktą iš kiekvieno JAV kariuomenės šarvuotame transporteryje „Stryker“ sumontuoto daviklio (jų yra 17), padeda transporto priemonių parkui sudaryti individualius techninės priežiūros planus ir aptikti ankstyvus gedimus. Ta pati sistema ateityje turėtų būti naudojama siekiant supaprastinti bei modernizuoti ir kitus logistikos procesus. Naudodama DI, „Watson“ leistų kariuomenės analitikams atsisakyti techninių užduočių ir padėtų parinkti optimaliausius atsarginių detalių transportavimo būdus. Šiuo metu septyni JAV kariuomenės logistikos palaikymo veiklos (angl. *Logistics Support Activity* – LOGSA) specialistai, išanalizuodami tik 10 proc. kariuomenės siuntų užklausų, kasmet sutaupo daugiau nei 100 mln. JAV dolerių [7]. Nesunku suskaičiuoti, kiek būtų galima sutaupyti, jei ši užduotis būtų patikėta sistemai „Watson“, kuri išanalizuotų 100 proc. visų užklausų.

DI atveria naujas galimybes logistikos ir planavimo srityse sparčiai ir efektyviai sprendžiant sudėtingas užduotis. Modernios DI paremtos sistemos padeda atrasti optimaliausius transportavimo būdus ir leidžia analitikams vietoj rutininių techninių užduočių koncentruotis į aukštesnio lygio strateginius sprendimus.

Pusiau autonominės ir autonominės transporto priemonės

DI sėkmingai diegiamas pusiau autonominėse ir autonominėse transporto priemonėse, tokiose kaip naikintuvai, bepiločiai orlaiviai, antžeminės transporto priemonės ir laivai. Šiose sistemose DI naudojamas aplinkos suvokimo, kliūčių identifikavimo, įvairių jutiklių duomenų susiejimo ir apdorojimo funkcijoms, navigacijai bei komunikacijai su kitomis transporto priemonėmis.

JAV karinių oro pajėgų programos „Loyal Wingman“ pratybų metu buvo sėkmingai išbandytas nepilotuojamas naikintuvas F-16 mišrioje rikiuotėje kartu su žmogaus pilotuojamais naikintuvais F-16 ir F-35. „Loyal Wingman“ technologija suteikia pilotui galimybę nepilotuojamam orlaiviui duoti bendrus nurodymus, pavyzdžiui, pulti arba suformuoti rikiuotę. Tačiau bepilotis orlaivis taip pat gali veikti ir autonomiškai, savarankiškai palaikydamas rikiuotę ir vykdydamas puolimo užduotis be tiesioginio žmogaus valdymo. Pirmajame pratybų etape, kuriame buvo imituojama antžeminė ataka, pagrindinis dėmesys buvo skiriamas skrydžiui rikiuotėje su pilotuojamu naikintuvu. Antrajame, sudėtingesniame, etape nepilotuojamas F-16 savarankiškai suplanavo ir įvykdė puolimo misiją, prisitaikydamas prie nenuspėjamų priešo oro gynybos veiksmų ir kompensuodamas tariamus pažeidimus bei ryšio su operatoriumi praradimą. Atlikus kelias modifikacijas, F-16 gali tapti visiškai autonominiu koviniu orlaiviu, galinčiu gabenti papildomą ginkluotę, stiprinti žmogaus pilotuojamų lėktuvų ugnies galią, nukreipti priešo gynybą ar net prisiimti dalį priešo ugnies. Galutinis „Loyal Wingman“ programos tikslas – sujungti penktosios kartos „Stealth“ naikintuvus su senesniais nepilotuojamais orlaiviais, siekiant padidinti smogiamąją galią oro kovose. Ši koncepcija taip pat gali būti pritaikyta ir kitoms lėktuvų bei bepiločių orlaivių konfigūracijoms [8].

JAV kariuomenė kuria ir išbando daugiafunkcį taktinį transportą (angl. *Multi Utility Tactical Transport* – MUTT), nuotoliniu būdu valdomas transporto priemones, kurios lydėtų karius mūšio lauke, gabentų didelius kiekius papildomos įrangos, taip pat savarankiškai atliktų įvairias užduotis [9], o autonominės robotizuotos kovinės transporto priemonės (angl. *Robotic Combat Vehicle* – RCV) galėtų atlikti žvalgybos, sprogmenų šalinimo ir kitas palaikymo funkcijas. Šios priemonės atliktų paramos modernesnėms kovos transporto priemonėms funkciją [10].

Daugiafunkcis taktinis transportas (MUTT)
Šaltinis: https://generaldynamics.uk.com/systems/land-systems/multi-utility-tactical-transport-mutt/

Robotizuota kovinė transporto priemonė (RCV)
Šaltinis: https://www.nationaldefensemagazine.org/articles/2022/10/7/army-robotic-combat-vehicle-advances

DARPA sukurtas eksperimentinis autonominis laivas „Sea Hunter“ gali savarankiškai plaukioti atviroje jūroje kelis mėnesius be pertraukų, vykdydamas nuolatinį povandeninių laivų stebėjimą, ir koordinuoti užduotis su kitais autonominiais laivais. Analitikai pabrėžia, kad šio laivo eksploatacijos išlaidos sudarytų tik apie 20 000 JAV dolerių per dieną, kai standartinio eskadrinio minininko su įgula eksploatavimo vertė – 700 000 JAV dolerių per dieną [11].

Autonominis laivas „Sea Hunter“
Šaltinis: https://wizvox.com/2018/02/13/darpa-sea-hunter-worlds-largest-autonomous-ship-transferred-to-u-s-navy/

Šiuo metu išbandomi ir kiti DI paremti pajėgumų didinimo būdai. Vienas iš jų – bendradarbiaujančių autonominių sistemų koncepcija, vadinama „Spiečiais“ (angl. *Swarming*). Ši technologija apima įvairių autonominių transporto priemonių bendradarbiavimą ir gali būti pritaikyta tiek dideliems nebrangių bepiločių orlaivių junginiams, skirtiems priešo gynybai įveikti, tiek mažesnių transporto priemonių būriams, kurie kartu atliktų ugnies palaikymo funkciją arba kurtų lokalizuotus navigacijos bei komunikacijos tinklus sausumos pajėgoms. 2016 m. JAV karinis laivynas sėkmingai išbandė šią technologiją: penkių autonominių laivų grupė 25 kv. km plote sulaikė „įsibrovusį“ laivą. Ateityje ši DI paremta technologija galėtų būti pritaikyta uostų apsaugai, povandeninių laivų medžioklei ar žvalgybos misijoms kartu su didesniais laivais [10].

Mirtinos autonominės ginklų sistemos (angl. *Lethal Autonomous Weapon System* – LAWS), ko gero, yra daugiausia diskusijų kelianti DI naudojimo sritis, nes ji susijusi su etiniais ir teisiniais aspektais – ar galima patikėti tik mašinai, be žmogaus dalyvavimo, panaudoti mirtiną jėgą? Autonominės ginklų sistemos naudoja jutiklius ir kompiuterinius algoritmus, kurie leidžia savarankiškai nustatyti taikinį, jį atakuoti ir sunaikinti be žmogaus valdymo. Autonominės ginklų sistemos atveria naujas perspektyvas karinėms operacijoms vietovėse, kuriose komunikacija yra sudėtinga arba išvis negalima ir kur neįmanoma naudoti įprastų sistemų. Šiuo metu nė vienos šalies kariuomenė oficialiai nėra įteisinusi autonominių ginklų sistemų naudojimo, nors nemažai valstybių, įskaitant JAV, Kiniją, Rusiją ir Jungtinę Karalystę, aktyviai tyrinėja ir kuria šias sistemas [10].

Kibernetinė erdvė

DI greičiausiai taps viena svarbiausių technologijų kibernetinių operacijų srityje. Įprastos kibernetinio saugumo priemonės jau nebespėja reaguoti į sparčiai kintančias grėsmes [12]. Įprasti saugumo įrankiai dažniausiai ieško jau žinomo kenkimo kodo atiti-

kmenų, tačiau įsilaužėliai gali lengvai apeiti esamas saugumo priemones, pakeisdami nedideles kodo dalis. Tuo metu DI sistemos, naudojančios mašininį mokymąsi, gali stebėti programinės įrangos veiksmus, aptikti ne tik žinomas, bet ir naujas grėsmes, greitai į jas reaguoti. 2016 m. DARPA organizuoto „Didžiojo kibernetinio iššūkio“ (angl. *Cyber Grand Challenge*) metu buvo pademonstruoti DI algoritmai, kurie per kelias sekundes savarankiškai aptiko, įvertino ir užtaisė saugumo spragas, užkirsdami kelią vienai iš besivaržančių komandų jomis pasinaudoti. Įprastai šis procesas užtruktų kur kas ilgiau [3, 10].

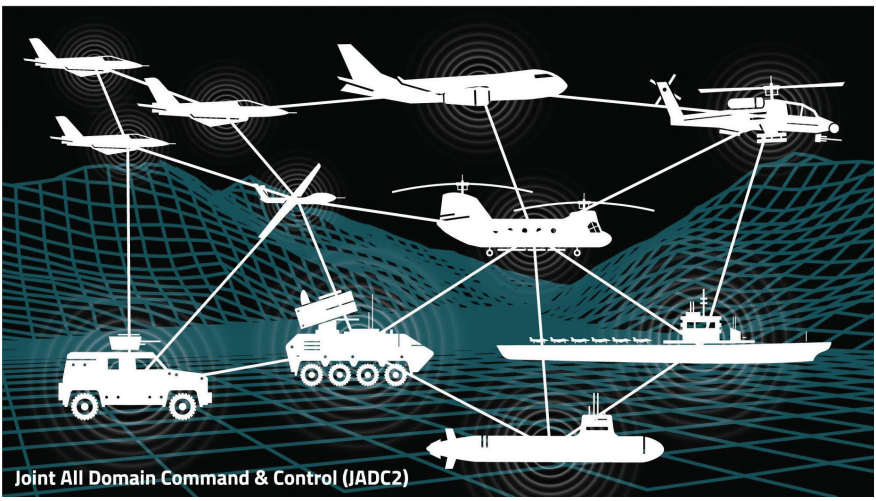
DI naudojamas kuriant itin tikroviškas nuotraukų, garso bei vaizdo įrašų klastotes, dar vadinamas *„deepfake“* (liet. *išmanioji* arba *sintetinė vaizdo klastotė*). Tokios klastotės kelia pavojų informaciniam saugumui ir gali būti naudojamos klastojant naujienas, paveikiant viešąją nuomonę, mažinant visuomenės pasitikėjimą ir šantažuojant diplomatus bei kitus aukšto rango pareigūnus. Kaip atsakas į šią grėsmę kuriami įrankiai, kurie automatiškai išanalizuotų ir aptiktų sintetines vaizdo klastotes bei užtikrintų vaizdinės žiniasklaidos integralumą.

DI technologijos nuolat tobulėja, ir tikėtina, kad ateityje jos sugebės apgauti kai kuriuos aptikimo įrankius, todėl būtina užtikrinti, kad šie įrankiai nuolat būtų tobulinami ir prisitaikytų prie technologinių pokyčių [10].

Vadovavimas ir kontrolė

Vis didėjantis karinių konfliktų tempas ir eksponentiškai augantys turimų duomenų kiekiai skatina kariuomenes kurti naujas vadovavimo ir valdymo sistemas. Senesnės vadovavimo ir kontrolės sistemos, kurios remiasi daug išteklių reikalaujančiomis procedūromis ir technologiškai ribotomis priemonėmis, dažniausiai orientuotomis į vieną sritį, nėra pritaikytos sudėtingiems ateitiems konfliktams. Tai turi neigiamos įtakos vadų informuotumui apie padėtį, sprendimų priėmimo spartai ir greitam pajėgų integravimui įvairiose srityse. Naudojant DI algoritmus, JAV kariuomenės ku-

riama Jungtinė visų sričių vadovavimo ir kontrolės sistema (angl. *Joint All Domain Command and Control* – JADC2) padėtų užtikrinti informuotumą apie padėtį, paspartintų sprendimų priėmimą ir supaprastintų centralizuotą vadovavimą oro, kosmoso, kibernetinės erdvės, sausumos ir jūrų pajėgoms. DI sujungtų visą šią informaciją į vieną ekraną, pateiktų išsamų draugiškų bei priešo jėgų vaizdą ir automatiškai ištaisytų įvesties duomenų nuokrypius. Tokio pobūdžio pažangi technologija padėtų vykdyti operacijas kovos lauke ir užtikrintų, kad ne tik transporto priemonės, bet ir orlaiviai, šaudmenys, palydovai, laivai, povandeniniai laivai, tankai ir žmonės būtų reikiamoje vietoje reikiamu laiku, persekiodami reikiamą taikinį ir veikdami sekundžių tikslumu [13].



JADC2 sistemos koncepcija
Šaltinis: https://www.eizorugged.com/wp-content/uploads/2023/01/JADC2_Graphic.jpg

JADO (angl. *Joint All Domain Operations*) koncepcija turėtų suteikti vadams prieigą prie informacijos, kuri leistų pasirinkti optimaliausią sprendimą vienu metu vykdomose ar vėliau planuojamose operacijose, išnaudojant netikėtumo veiksnį ir greitą pajėgumų integravimą visose srityse, siekiant įgyti fizinį bei psichologinį pranašumą ir daryti įtaką bei kontroliuoti operacinę aplinką. 2019 m.

sistema buvo sėkmingai išbandyta karo pratybose, imituojant priešininko paleistos sparnuotosios raketos scenarijų. Karinių oro pajėgų ir Karinio jūrų laivyno orlaiviai (F-22 ir F-35), Karinio jūrų laivyno eskadrinis minininkas, kariuomenės radiolokacinė sistema „Sentinel“, mobilioji artilerijos sistema, taip pat komercinių palydovų ir antžeminiai jutikliai rinko, analizavo ir dalijosi duomenimis realiuoju laiku ir pateikė išsamesnį operacinės aplinkos vaizdą. Pranešama, kad 26 iš 28 išbandytų pajėgumų buvo funkcionalūs [13]. Vis dėlto ne visų požiūris į naujas sistemas yra toks optimistinis. Kai kuriems analitikams kyla klausimų dėl pačios technologijos: ar ji yra įperkama ir ar realu įdiegti tinklą, kuris saugiai ir patikimai sujungtų visus jutiklius su šauliais ir užtikrintų vadovavimą bei kontrolę pavojingoje elektroninio karo aplinkoje.

Ateities perspektyvos

Pasak Carlo von Clausewitzo, karo prigimtis – „jėgos veiksmas, skirtas priversti priešą paklusti mūsų valiai“ – visuomet išliks tokia pati. Tačiau karo pobūdis, tai yra, kaip kariaujama konkrečiu laiku ir vietoje, priklausys nuo tuo metu vyraujančių aplinkybių ir istorinio konteksto. Kaip parako ar aviacijos atsiradimas iš esmės pakeitė karo pobūdį praeityje, taip DI ateityje gali iš esmės pakeisti tai, kaip bus kariaujama ateityje. Tai gali įvykti greičiau, nei daugelis suvokia. DI nėra tik pavienė technologija. Tai technologijų grupė, kurią galima pritaikyti įvairiose srityse. Šios technologijos gali paspartinti sprendimų priėmimą, suteikti naujų galimybių karinei analizei ir didinti kovinį potencialą. DI naudojimas kare gali padaryti reikšmingą, gal net ir transformuojantį poveikį karybos evoliucijoje [3].

Šiuo metu DI technologijos tobulėja gana sparčiai ir yra pritaikomos įvairiose srityse, tačiau kol kas nėra aišku, kiek tai truks ir koks bus vystymosi tempas. Kai kurie specialistai sutelkia dėmesį į technologijas, kurias bus galima pritaikyti artimiausiu metu. Kiti analizuoja „superintelekto“ sistemų perspektyvas, kurios galėtų atsirasti tik po kelių dešimtmečių arba toks scenarijus gali apskritai

neišsipildyti. Skirtingos DI plėtros perspektyvos turės skirtingas implikacijas karo etikai. Jei DI tobulės sparčiai ir bus pasiekta didelė pažanga objektų atpažinimo, sprendimų priėmimo, paramos, kibernetinio saugumo ir kitose gynybai svarbiose srityse, tuomet karinės institucijos suskubs visapusiškai integruoti šias technologijas. Pagal tokį scenarijų itin svarbus vaidmuo karyboje tektų autonominėms sistemoms, kurių veikimo greitis galėtų viršyti žmogaus galimybes šias sistemas valdyti ir apriboti. Tokio spartaus vystymosi atveju atsirastų etinės, operacinės ir strateginės rizikos, kurias reikėtų suvaldyti. Kita vertus, DI evoliucija gali susidurti su techninėmis kliūtimis, kurios pristabdytų tolesnį technologijų vystymą ir finansavimą, kaip jau ne kartą yra įvykę praeityje, kai progresas sustoja ir prasideda ilgas sąstingio laikotarpis, vadinamas „dirbtinio intelekto žiema“. Tokiu atveju etikos klausimai, susiję su karu, išliktų tokie patys. Nors jie nėra nereikšmingi, situacijos neapsunkins autonomiškai veikiančios mašinos, nes karo veiksmus ir toliau kontroliuos žmonės. Vis dėlto labiausiai tikėtinas scenarijus, kad DI progresas vyks tolygiai, o karinės institucijos sieks jį pritaikyti įvairiose srityse. Tokiu atveju DI kels naujų etinių klausimų, tačiau jo vystymosi tempas bus pakankamai nuosaikus, kad būtų galima sąmoningai apriboti ekstremalias rizikas. Tai suteiks laiko kruopščiai analizei, leidžiančiai nustatyti geriausius būdus, kaip užtikrinti prasmingą žmogaus vaidmenį kontroliuojant karines DI sistemas [3].

Bibliografija

1. Ross, P., Maynard, K. Towards a 4th Industrial Revolution. In: *Intelligent Buildings International,* 2021, Vol. 13, Issue 3, p. 159–161. Prieiga per internetą: https://doi.org/10.1080/17508975.2021.1873625

2. Haenlein, M., Kaplan, A. A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review,* 2019, 61(4), 5–14.

3. Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., Grossman, D. Military Applications of

Artificial Intelligence. Santa Monica: RAND Corporation, 2020.

4. Wu, X., Qin, D., Li, Y. Challenges and Inspirations of AI and Related Technologies in Intelligence Analysis. *2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC),* 2022, Vol. 10, p. 451–455.

5. Hedberg, S. R. DART: Revolutionizing Logistics. *IEEE Intelligent Systems,* 2002, 17(3), p. 81–83.

6. Weisgerber, M. Defense Firms to Air Force: Want Your Planes' Data? Pay Up. 2017. Prieiga per internetą: http://www.Defenseone.Com/Technology/2017/09/Military-Planes-Predictivemaintenance technology/141133

7. Stone, A. Army Logistics Integrating New AI, Cloud Capabilities. *C4ISRNET,* 2017, September 14.

8. Axe, D. US Air Force Sends Robotic F-16s into Mock Combat. *National Interest,* 16, 2017. Prieiga per internetą: https://nationalinterest.org/blog/the-buzz/us-air-force-sends-robotic-f-16s-mock-combat-20684

9. Houser, K. The Marines' Latest Weapon Is a Remote-Controlled Robot With a Machine Gun. 2017. Prieiga per internetą: https://futurism.com/the-marines-latest-weapon-is-a-remote-controlled-robot-with-a-machine-gun

10. Sayler, K. M. Artificial Intelligence and National Security. *Congressional Research Service,* 2020, R45178.

11. Turner, J. Sea Hunter: Inside the US Navy's Autonomous Submarine Tracking Vessel. 2018. Prieiga per internetą: https://www.naval-technology.com/features/sea-hunter-inside-us-navys-autonomous-submarine-tracking-vessel/

12. Lyle, A. National Security Experts Examine Intelligence Challenges at Summit. US Department of Defense, 2016, September 9. Prieiga per internetą: https://www.defense.gov/News/News-Stories/Article/Article/938941/national-security-experts-examine-intelligence-challenges-at-summit/

13. Smagh. Defense Capabilities: Joint All Domain Command and Control. 2020. Prieiga per internetą: https://crsreports.congress.gov/product/pdf/IF/IF11493/2