Mojca Pešec

DOI:10.33179/BSV.99.SVI.11.CMC.22.1.7

VPLIV RAZVOJA UMETNE INTELIGENCE NA NACIONALNO VARNOST

IMPACT OF ARTIFICIAL INTELLIGENCE DEVELOPMENT ON NATIONAL SECURITY

Povzetek Razvoj umetne inteligence bo pomembno vplival na mednarodno varnost in uporabo vojaškega instrumenta moči. Priprava na posledice, ki jih bo prinesel razvoj umetne inteligence, je ena od pomembnejših nalog za strokovnjake in odločevalce na področju nacionalne varnosti. Pri razvoju vojaških zmogljivosti se umetna inteligenca vključuje v obveščevalne, opazovalne in aplikacije za potrebe izvidovanja ter nadziranja, v logistiko, kibernetske operacije, informacijske operacije, sisteme poveljevanja in kontrole, polavtonomna in avtonomna vozila ter ubojne avtonomne oborožitvene sisteme.Revolucija na področju umetne inteligence se ne bo zgodila jutri. Politike, ki bodo pripravljene vnaprej, in znanje, ki ga bodo posedovali oblikovalci teh politik in odločevalci, lahko pomagajo pri upravljanju neznank, ki so pred nami.

Ključne besede ***Umetna inteligenca, nacionalna varnost, vojaški instrument moči, vojaške zmogljivosti, odločevalci.***

Abstract The development of artificial intelligence will have a significant impact on international security and the use of a military instrument of power. One of the most important tasks for national security professionals and decision makers is thus to prepare for the consequences of artificial intelligence development. In the development of military capabilities, artificial intelligence is integrated into intelligence, observation, control and reconnaissance applications, as well as into logistics, cyber operations, information operations, command and control systems, semi-autonomous and autonomous vehicles, and lethal autonomous weapon systems. The artificial intelligence revolution is not going to happen tomorrow. Therefore, pre-prepared policies and the knowledge shared by policy- and decision makers can help us manage the unknowns ahead.

Key words ***Artificial intelligence, n ational security, m ilitary i nstrument o f power, military capabilities, decision-makers.***

Uvod

Strokovnjaki po vsem svetu opozarjajo, da smo v pospeševalniku globalne revolucije na področju umetne inteligence (Artificial Intelligence) in strojnega učenja (Machine Learning). Oba dejavnika bosta pomembno vplivala tudi na prihodnje gospodarsko in vojaško tekmovanje med državami.

Prihodnost, v kateri bo vse več nalog in odločitev prepuščenih pametnim strojem (Intelligent Machines), je za večino ljudi težko predstavljiva. Na naše predstave največkrat vplivajo podobe o prevladi strojev nad ljudmi iz znanstvenofantastičnih filmov in knjig, v katerih nas bodo zasužnjili, ubili ali pa bodo prevzeli naše službe. To so najbolj črni scenariji, toda pametni stroji lahko na družbo vplivajo tudi pozitivno. Njihov razvoj bo najverjetneje povzročil novo industrijsko revolucijo. Izboljšal konkurenčnost podjetij. Omogočil napredek na področju medicine. Omogočil nove načine učenja. Umetna inteligenca lahko spremeni razmerje moči in najpomembnejše gradnike globalne ekonomije. Pričakujemo lahko, da bo povzročila tudi politične in družbene spremembe, tako kot sta jih prva in druga industrijska revolucija.

Tiste države, ki bodo imele dostop do najboljših podatkov, najbolj sposobnih računalnikov, ki bodo poskrbele, da bodo imele najbolj izobražene in inovativne kadre, ki bodo razvijali tehnologije, in odločevalce, ki bodo razvoj na tem področju spodbujali, bodo tekmovale v tekmi za prestiž na področju umetne inteligence.

Namen našega prispevka je, da predstavimo razvoj tehnologij in sistemov umetne inteligence in njihov vpliv na nacionalno varnost ter uporabo vojaškega instrumenta moči.

Revolucija na področju umetne inteligence se ne bo zgodila jutri, zagotovo pa se bo razvijala v različne smeri in nekatere od teh bodo lahko presenečenje za vse. Nemogoče je predvideti vse spremembe, ki jih bo prinesla.

Zato bo priprava na posledice, ki jih bo prinesel razvoj umetne inteligence, ena od pomembnejših nalog za strokovnjake in odločevalce na področju nacionalne varnosti. Priprava politik in znanje, ki ga bodo posedovali oblikovalci teh politik in odločevalci, bo pomembno in bo pomagalo pri upravljanju neznank, ki so pred nami. Razvoj umetne inteligence pomeni namreč številne prednosti, pa tudi tveganja. V kontekstu nacionalne varnosti in še posebej pri uvajanju sistemov umetne inteligence v vojsko je treba zagotoviti, da so odločevalci s tehnologijo seznanjeni, predvsem pa, da celovito razumejo morebitne učinke njene uporabe.

V članku predstavljamo temeljna znanja in terminologijo s področja umetne inteligence. Osvetlili smo trenutni in predviden prihodnji razvoj umetne inteligence, tveganja in priložnosti, ki jih predstavlja, ter njen vpliv na nacionalno varnost in uporabo vojaškega instrumenta moči. Pri tem smo uporabili kvalitativno analizo pisnih virov ter opisno (deskriptivno) metodo družboslovnega raziskovanja, s pomočjo katere smo predstavili primer razvoja umetne inteligence v oboroženih silah ZDA.

1 TERMINOLOGIJA IN DEFINICIJE

Inteligenca je (merljiva) sposobnost prilagajanja okolju in reševanja problemov.

O tem, kaj je umetna inteligenca, so znane različne definicije, ki izvirajo iz različnega pojmovanja človekove inteligence (sposobnost razmišljanja, sklepanja, učenja in komuniciranja) in tega, kaj pričakujemo od stroja (računalnika, računalniškega sistema).

Umetna inteligenca (UI) je znanstvena disciplina, ki je osredotočena na razvoj inteligentnih sistemov oziroma pametnih strojev. Inteligenca v tem kontekstu je merilo sposobnosti sistema, da določi najboljšo smer delovanja za dosego cilja v različnih okoljih. Področje umetne inteligence ima več poddisciplin in metod, s katerimi razvijajo inteligentno vedenje. Umetna inteligenca in strojno učenje, ki je metoda discipline umetne inteligence, omogočajo ustvarjanje različnih, posebnih strojev, katerih namen je izvajanje uporabnih kognitivnih nalog. To so pametni stroji (Buchanan, Miller, 2017, str. 5).

Zgodnji sistemi umetne inteligence so bili t. i. ekspertni sistemi, ki so temeljili na točno določenih pravilih. Računalniški program je sledil skupini posebnih navodil o tem, kako naj se odziva v neki situaciji. Novi UI-sistemi omogočajo bolj sofisticirano delovanje. Strojno učenje omogoča algoritmom, da se učijo iz podatkov in razvijejo rešitve. Ti vedno pametnejši stroji se lahko uporabljajo v različne namene: za analiziranje podatkov, simulacijo, preverjanje, nadzor, diagnostiko, iskanje vzorcev in odstopanj, predvidevanje trendov, napovedovanje. Strojno učenje torej podpira proces odločanja (Buchanan, Miller, 2017, str. 5–6).

Strokovnjaki delijo UI-sisteme na močne in šibke. Šibki sistemi so ozko specialistično omejeni na določeno področje oziroma domeno delovanja, medtem ko naj bi bili močni UI-sistemi, ki se še razvijajo, sposobni svoje znanje uporabljati širše. Povedano bolj enostavno: trenutno stroji ne zmorejo presoje, ki ljudem omogoča prožnost pri izvajanju in prehajanju na izvajanje različnih nalog. Omejitve trenutnih sistemov UI lahko povzročijo, da ti ne bodo zmogli izvesti naloge, če so postavljeni zunaj konteksta, za katerega so bili oblikovani. Sistem, ki lahko neko nalogo izvede veliko bolje kot človek, bo drugo nalogo, za katero so se spremenili pogoji delovanja, za katere je bil oblikovan, izvedel slabo ali pa sploh ne.

Sistemi UI se lahko definirajo tudi kot avtonomni, podporni in svetovalni sistemi. Avtonomni sistemi samostojno načrtujejo in izvajajo aktivnosti v realnem svetu, na primer roboti za razminiranje. Podporni sistemi sodelujejo pri sprejemanju odločitev, vendar ne morejo delovati samostojno. Svetovalni sistemi posredujejo informacije, s pomočjo katerih je odločanje učinkovitejše in uspešnejše.

Strojno učenje predstavlja zelo uspešen pristop za oblikovanje inteligentnega vedenja. Ko dobijo cilj, stroji skozi proces učenja iz podatkov prilagodijo svoje vedenje tako,

da optimizirajo delovanje na način, ki jim omogoča dosego cilja (Buchanan, Miller, 2017, str. 8).

Strojno učenje se uporablja na različnih področjih (vsakodnevno življenje, ekonomija, medicina, različne raziskave, bančništvo idr.) za igranje iger, analiziranje podatkov, oblikovanje baz znanja, prepoznavanje, napovedovanje, prepoznavanje slik, jezika.

Stroji se učijo na različne načine. Strojno učenje temelji na opisovanju pojavov iz podatkov, zato so podatki (data) zelo pomembni za proces strojnega učenja. Metode, s katerimi se izvaja strojno učenje, so nadzorovano učenje, nenadzorovano učenje, učenje relacij in spodbujevalno učenje. Rezultati strojnega učenja so lahko pravila, funkcije, relacije ipd. (Buchanan, Miller, 2017, str. 9).

Nadzorovano učenje (supervised learning) za učenje uporablja označene podatke. Algoritem se poskuša naučiti osnovnega koncepta iz množice različnih označenih vzorcev (Hiršman M., 2014, str. 24). Sprejema lahko milijone različnih označenih vzorcev, na primer slik. Algoritem se nato nauči razlikovati med različnimi slikami in tako prepoznavati različne kategorije (Buchanan, Miller, 2017, str. 5–6). Če stroj dobi na primer zadosti slik jabolk in paradižnikov, se bo naučil, v čem se sadeža, ki sta oba okrogla in z gladko svetlečo površino, rdeča, med seboj razlikujeta in tako prepoznati oziroma razlikovati jabolko od paradižnika, čeprav nista označena. Stroji so že leta 2016 presegli človekovo sposobnost v prepoznavanju in klasifikaciji slik (AI Index, 2019, str. 26).

Pri nenadzorovanem učenju (unsupervised learning) so vsi vzorci označeni in uporabljeni za učenje. Algoritem poskuša najti neko urejenost ali strukturo (Hiršman M., 2014, str. 24) tudi med neoznačenimi slikami jabolk in paradižnikov. Tudi brez imen so stroji sposobni razvrstiti podatke v zbirke ali kategorije na podlagi vzorcev znotraj podatkov. Tako kot lahko ljudje prepoznamo določene vzorce vedenja in pravil tudi v situacijah, ki jih ne poznamo, lahko stroji najdejo odstopanja ali predvidijo prihodnje vedenje na podlagi analiziranja podatkov (Buchanan, Miller, 2017, str. 9).

Spodbujevalno učenje (reinforcment learning) za učenje stroja uporablja povratno poročilo iz okolja (Buchanan, Miller, 2017, str. 9–11). Tako kot se ljudje naučimo iz izkušenj, se UI-sistemi naučijo, ali je njihovo delovanje pri doseganju cilja uporabno oziroma škodljivo. Tisti, ki igrate šah s pametnimi stroji, veste, da ti izpopolnjujejo svojo igro tako, da prepoznajo, da nekatere poteze zagotavljajo boljši rezultat.

Globoko učenje (deep learning) pri učenju stroja uporablja nevralna omrežja. Ta omrežja so ohlapen približek bioloških nevronov in uporabljajo vrsto umetnih nevronov, ki so povezani v omrežje v več plasteh. Vhodni podatki prihajajo v omrežje na eni strani in prehajajo čez različne plasti umetnih nevronov do izhoda (Buchanan, Miller, 2017, str. 14–15). Vhodni podatek za slikovno prepoznavo je na primer vsaka posamezna slikovna točka slike paradižnika. Izhod nevralnega omrežja

je poimenovanje slike – paradižnik. Nevralna omrežja uporabljajo za učenje vse zgoraj naštete oblike učenja in so danes že v široki uporabi za prepoznavanje slik, vse do predvidevanj, kakšen bo zaključek določenega procesa, na primer zdravljenja. Nevralna omrežja skrbijo za Googlove podatkovne centre, so v vojaških in civilnih dronih ipd. (Svet elektronike, str. 2019).

2 UPORABNOST UMETNE INTELIGENCE

UI-sistemi so v naših življenjih prisotni že desetletja. Toda nedavni napredek na področju obsežnih podatkov (big data), sposobnosti računalniške obdelave in izboljšani algoritmi so zmogljivosti UI-sistemov bistveno povečali.

Vse več naprednih UI-sistemov se iz laboratorijev uvaja v vsakodnevno življenje. Prepoznavanje slik (image recognition) je že davno preseglo človekove sposobnosti. Toda strokovnjaki zagovarjajo, da za nekatere UI-sisteme ni nujno, da bi dosegli nivo »superčloveka«. V mnogih primerih so uporabni že zato, ker so cenejši, hitrejši in se jih lahko uporabi na načine, ki ne zahtevajo enakovrednega obsega, kot jih lahko omogočijo človekove izkušnje.

Danes se UI uporablja na področjih razvrščanja podatkov (data classification), prepoznavanja odstopanj (anomaly detection), predvidevanja oziroma napovedovanja (predicition) in optimizacije (optimization) (Li, 2019).

Razvrščanje podatkov je proces, v katerem UI-sistem pomaga razvrščati različne vhodne podatke.

Prepoznavanje odstopanj je proces, v katerem se identificirajo nepričakovani ali redki predmeti, dogodki, opazovanje, podatki oziroma zbir podatkov, ki se razlikujejo od določene norme oziroma odstopajo od večine drugih podatkov.

Predvidevanje je proces, v katerem UI-sistemi pregledujejo vzorce v večjem številu podatkov in proizvajajo statistično predvidevanje o prihodnjem vedenju. Predvidevanje, podprto s sistemi UI, se danes že široko uporablja pri napovedih vremena, v medicini in priporočilih, ki jih dobimo, ko pregledujemo različne iskalnike, na primer Amazon ipd.

UI-sistemi se lahko uporabijo za optimizacijo delovanja kompleksnih sistemov in nalog, na primer na področju izboljšanja energetske učinkovitosti.

UI lahko zagotovi tudi oblikovanje strojev, ki lahko delujejo bolj avtonomno, z več svobode in izvajajo naloge sami. Avtonomnost ima več prednosti: avtomatizacijo izvajanja posameznih nalog in nalog v večjem obsegu, hitrejše, bolj natančno, bolj zanesljivo in samostojno delovanje. Avtomatizacija zagotavlja, da lahko nekdo, ki je manj izurjen, opravlja naloge podobno kot nekdo, ki je visoko izurjen, in sicer na način, da se ustrezna ekspertiza vnese v stroj.

Danes je mogoče računalniške programe dobiti praktično zastonj, kar omogoča, da lahko z avtomatizacijo uvedemo ekspertizo v večjem obsegu. Z avtomatizacijo lahko tako naloge, ki bi jih ljudje lahko izvajali v manjšem obsegu, stroji izvajajo v večjem obsegu.

Avtomatizacija zagotavlja, da se lahko naloge izvajajo izjemno hitro, natančno in zanesljivo.

UI-sistemi lahko opazujejo podatke. ne da bi se utrudili ali izgubili pozornost ter neodvisno in brez povezav z ljudmi, kar lahko traja tudi dalj časa.

V prihodnosti lahko pričakujemo, da bodo stroji vedno bolj avtonomni in da bodo vedno več različnih nalog izvajali samostojno.

3 OMEJITVE IN RANLJIVOST SISTEMOV UMETNE INTELIGENCE IN STROJNEGA UČENJA

UI-sistemi imajo še vedno premalo sposobnosti, da bi razumeli kontekst za svoje vedenje, prožnost, da se prilagodijo novim okoliščinam, ki so zunaj parametrov, ki določajo njihovo delovanje, in uporabo tega, kar ljudje označujemo kot »smiselno« ali »kmečko logiko«.

UI-sistem, ki prepoznava slike, lahko pravilno prepoznava objekte v neki situaciji, ne more pa oblikovati poročila o tem, kaj se dogaja. Prepozna lahko človekov obraz, premikanje telesa, ne more pa zanesljivo povedati, kaj je motivacija za neko človekovo vedenje. UI v tej fazi razvoja dosega t. i. »idiot-savant« stopnjo inteligence.

UI-sistemi so ranljivi in imajo veliko varnostnih zadržkov. Ti so še posebej pomembni za uporabo na področju nacionalne varnosti, pri čemer so napake sistema ali vdor nasprotnika v sistem nevarni.

Trenutni sistemi UI ne morejo razumeti širšega konteksta, v katerem izvajajo določeno aktivnost. Svojega vedenja ob spremembi konteksta ne morejo ustrezno spremeniti. Zato je človekov nadzor, ki lahko zaustavi ali spremeni aktivnost sistema UI ob spremembi okolja, nujen.

Zaradi zapletenosti sistemov UI je njihovo vedenje težko predvidevati vnaprej. To je še posebej problematično, če so UI-sistemi usmerjeni k doseganju cilja in delujejo v realnem okolju. Prednost tega, da tak sistem sam določa najboljšo pot za dosego cilja, je lahko problematična, če je ta pot zunaj meja pričakovanega ali zaželenega.

Nekatere metode, ki jih uporabljajo sistemi UI, še posebej globoka nevralna omrežja, so težko razumljive. Za razširitev in varnost uporabnosti je pomembno,

da uporabniki UI-sistema razumejo vse metode, ki jih sistem uporablja za izvajanje neke aktivnosti.

Učeči se stroji imajo prav tako vrsto varnostnih težav, do katerih prihaja v fazi učenja. Če njihov cilj ali operativna funkcija nista pravilno opredeljena, lahko stroj v procesu strojnega učenja pride do napačnega zaključka o tem, kaj je njegov cilj oziroma funkcijo izvede napačno.

Sistemi UI so prav tako občutljivi na sistemske napake, ki izvirajo iz zapletenih interakcij med posameznimi elementi sistema. Sistemi lahko vsebujejo odstopanja od standardov ali tako imenovani predsodek (bias), ki odraža posreden ali neposreden predsodek njegovega oblikovalca. Omeniti velja še napake, ki izvirajo iz interakcije med sistemom in človekom, če ta ne razume omejitev sistema ali povratnih informacij, ki jih sistem daje.

Akterji, ki želijo izkoristiti pomanjkljivosti oziroma ranljivosti sistemov UI, lahko manipulirajo z naštetimi omejitvami in ranljivostmi sistemov UI ter učečih se strojev in ustvarijo nove kategorije tveganj. Lahko se seznanijo z delovanjem sistemov UI in poskušajo na primer »zastrupiti« podatke v procesu učenja oziroma vnesti lažne podatke ali izvesti t. i. prikriti napad (spoofing attacks) in tako povzročiti, da se stroj nauči napačnega vedenja.

Ranljivosti sistemov UI in učečih se strojev pomeni za nacionalno varnost velik izziv. Napake imajo lahko namreč težke in obsežne posledice. Izziv je še večji v razmerah sovražnosti, pri čemer lahko pričakujemo, da bodo ranljivosti sistemov UI in učečih se strojev poskušali izkoristiti tako državni kot tudi nedržavni akterji.

4 RAZVOJ UMETNE INTELIGENCE V KONTEKSTU NACIONALNE VARNOSTI (PRIMER RAZVOJA UI V OBOROŽENIH SILAH ZDA)

Umetna inteligenca je in bo uporabna na različnih področjih nacionalne varnosti. UI bo v prihodnosti vključena v vseh večjih sistemih, ki podpirajo delovanje obrambnega sistema.

Ameriško obrambno ministrstvo preučuje številne in različne aplikacije umetne inteligence. Razvoj umetne inteligence je v pristojnosti raziskovalnih organizacij (npr. DARPA[1]) in posameznih vojaških zvrsti (kopenske vojske, letalstva, mornarice in marincev). Posamezni projekti in pobude, ki stroškovno presegajo 15 milijonov dolarjev letno, se koordinirajo prek centralne ustanove JAIC (Joint Artificial Inteligence Center), ki spremlja razvoj projektov, povezanih z UI na nacionalni ravni. Tako se naslavljajo tudi najbolj nujne operativne zahteve vojske.

[1] *DARPA (The Defense Advanced Research Projects Agency) je agencija ameriškega obrambnega ministrstva, ki je odgovorna za razvoj najnovejših tehnologij za potrebe ameriške vojske.*

UI je danes že vključena v številne aplikacije, ki omogočajo izvajanje obveščevalnega delovanja, opazovanje, izvidovanje in nadziranje. Podpira logistično delovanje, kibernetske operacije, informacijske operacije, sisteme poveljevanja in kontrole, delovanje delno avtonomnih[2] in avtonomnih vozil (semi – and authonomous) ter ubojnih avtonomnih oborožitvenih sistemov.

Projekt Maven vsebuje avtomatizirano obdelavo obveščevalnih podatkov in podpira koalicijsko operacijo proti DAESH (Weisgerber, 2017).

Ameriško letalstvo že uporablja t. i. vzdrževanje na podlagi predvidevanja (predictive aircraft maintenance). Podoben sistem, Watson, se uvaja za vzdrževanje bojnih vozil kopenske vojske Stryker. IBM sistem Watson bo analiziral pridobivanje in distribucijo nadomestnih delov, s čimer želijo določiti najbolj časovno in cenovno učinkovite postopke za dobavo nadomestnih delov za različne sisteme in vozila za potrebe ameriške kopenske vojske.

Strokovnjaki napovedujejo, da bo ključna tehnologija UI tista, ki bo izboljšala kibernetske operacije. Kibernetska orodja, ki so podprta z UI, lahko na podlagi le enega algoritma izvajajo kibernetsko obrambo in kibernetski napad.

UI omogoča oblikovanje izjemno realističnih fotografij, avdio in video ponaredkov ali t. i. globokih ponaredkov[3] (deepfake), ki jih lahko sovražnik uporabi kot del informacijske operacije. Tehnologija globokih prevar je lahko uporabljena za širjenje lažnih novic, vplivanje na javno mnenje, povzročanje nezaupanja javnosti in kot sredstvo za izsiljevanje diplomatov. V preteklosti so strokovnjaki lahko te prevare odkrili, toda vedno bolj sofisticirana tehnologija bo delo otežila tudi najbolj sposobnim forenzičnim analitikom.

4.1 RAZVOJ UI NA PODROČJU OBVEŠČEVALNIH ZADEV, OPAZOVANJA IN IZVIDOVANJA (ISR)

V ameriški vojski se zavedajo, da bo UI še posebej uporabna na področju obveščevalnih zadev, opazovanja in izvidovanja (ISR).

Večzvrstna funkcijska skupina za algoritemsko vojskovanje (The Algoritmic Warfare Cross-Functional Team), bolj znana kot projekt Maven, je do nedavnega predstavljala osrednjo integracijsko točko za vse projekte UI na obrambnem ministrstvu.

Projekt je bil uveden leta 2017, ukvarjal pa se je s hitrim vključevanjem UI v takratne obrambne sisteme in predstavljanjem potenciala, ki ga ima tehnologija.

---

[2] *Avtonomno v najbolj enostavnem jeziku pomeni brez centralnega nadzora. Avtonomno sredstvo uporablja podatke, ki jih zbira v določeni situaciji, izvede preračunavanje, definira možnosti in sprejme razumno odločitev skladno s cilji, ki so mu bili določeni kot njegov namen.*

[3] *Globoki ponaredek je zamenjava fotografije oziroma podobe ene osebe z drugo idr. na sintetičnem mediju oziroma mediju, ki je oblikovan ali spremenjen s pomočjo algoritma.*

Danes projekt Maven prehaja pod okrilje centralne ustanove JAIC in vsenacionalne pobude z imenom National Mission Initiative. Prva faza projekta ameriškega obrambnega ministrstva Maven vsebuje avtomatizirano obdelavo obveščevalnih podatkov in podpira koalicijsko operacijo proti DAESH. Projekt Maven združuje računalnikov pogled in algoritem učečega se stroja pri zbiranju obveščevalnih podatkov v obveščevalne celice, ki pregledujejo posnetke brezpilotnega plovila in avtomatično identificirajo sovražne aktivnosti, ki nato postanejo tarča. Ta zmogljivost naj bi nadomestila človekovo pregledovanje posnetkov, ki zdaj traja veliko časa, in analistom omogočila, da lahko sprejmejo hitrejše in učinkovitejše odločitve na podlagi istih podatkov (Corrigan, 2017).

Obveščevalne agencije razvijajo algoritme za prepoznavanje govora v več jezikih v hrupnem okolju, sisteme UI, ki analizirajo geolokacijske posnetke in zagotavljajo spremljajoče metapodatke, združujejo D-2 posnetke v 3-D modele ipd.

4.2 Umetna inteligenca na področju vojaške logistike

UI ima prihodnost tudi na področju vojaške logistike. Ameriško letalstvo jo uporablja za napovedovanje potrebnega vzdrževanja letal. Namesto da bi se popravilo letala izvajalo takrat, ko se nekaj pokvari ali pa na podlagi standardiziranega urnika letalskega vzdrževanja, ki obsega vzdrževanje vseh letal v floti, ameriško letalstvo preizkuša pristop, ki ga podpira UI. Ta ustvarja urnike vzdrževanja, ki so oblikovani za potrebe vsakega letala. Tak pristop trenutno uporablja F-35 ALIS (Autonomic Logistic Information System), ki v realnem času izvzema podatke iz senzorjev v letalskem motorju in iz drugih sistemov na letalu ter jih pošilja v napovedovalni (predictive) algoritem, ki določa, kdaj je treba letalo pregledati ali zamenjati določen letalski del (Lopez, 2019).

V ameriški kopenski vojski je LOGSA (Army's Logistics Suppport Activity) s pomočjo IBM-ovega Watsona razvila podoben pristop pri vzdrževanju vozil Stryker. Na vozilu je 17 senzorjev, s pomočjo katerih se napove potreben pregled ali zamenjava delov vozila. Drugi projekt, ki poteka s pomočjo Watsona od leta 2017, je analiziranje dobavnih poti za nadomestne dele, pri čemer poskušajo zagotoviti oskrbo, ki bo časovno in finančno najbolj učinkovita. Trenutno to nalogo opravljajo analitiki, ki so z analizo približno 10 odstotkov zahtev za oskrbo ameriški vojski prihranili okoli 100 milijonov ameriških dolarjev na leto. Watson naj bi vojski zagotovil analiziranje vseh (100-odstotno) zahtev, kar naj bi kratkoročno pomenilo velik prihranek (Stone, 2017).

4.3 Umetna inteligenca in kibernetske operacije

Zanašanje na obveščevalne podatke, ki so proizvod procesa, ki ga izvaja človek, v kibernetski domeni vojskovanja pomeni, da imamo slabo strategijo. Količina aktivnosti, ki jih moramo danes razumeti, in kompleksnost, s katero se je treba spopadati, kadar poskušamo prepoznati določene povezave in prepoznati ter

razvozlati omrežja, je tako velika, da smo vedno v zaostanku, trdijo strokovnjaki (M. Rogers, 2016).

Konvencionalna kibernetska orodja pri odkrivanju zlonamernih kod iščejo pretekle podobnosti. To pomeni, da lahko hekerji[4] modificirajo le majhen del te kode in tako zaobidejo obrambo. Orodja, ki jih uporabljajo UI, se lahko naučijo, da odkrijejo nepravilnosti in širše vzorce aktivnosti v omrežju in tako predstavljajo celovitejšo in bolj dinamično oviro pred napadom (Rosenberg, 2017).

Kibernetske operacije, podprte z UI, bodo najverjetneje najpomembnejša tehnologija, ki bo podprla vojaške kibernetske operacije.

Leta 2016 predstavljena tehnologija na dogodku z naslovom Cyber Grand Challenge je prikazala potencialno moč, ki jih kibernetskim orodjem daje UI. Na tekmovanju so sodelujoči razvijali algoritme UI, ki naj bi avtonomno odkrili, ocenili in popravili ranljivosti določene programske opreme (software), preden bi druga tekmovalna skupina te ranljivosti izkoristila. Algoritmi UI so ranljivosti lahko odkrili in popravili v sekundah. Proces brez pomoči UI bi trajal mesece. Prikaz je omogočil vpogled v sposobnost UI ne le z vidika izjemne hitrosti, ki jo omogoča kibernetskemu orodju, temveč tudi potencialno sposobnost, da samo en algoritem izvaja obrambo in napad hkrati (DARPA, 2016). Tovrstne zmogljivosti lahko zagotovijo občutno prednost v prihodnjih kibernetskih operacijah.

4.4 Informacijske operacije

UI omogoča oblikovanje izjemno realističnih fotografij, avdio in video ponaredkov ali t. i. globokih ponaredkov, ki jih sovražnik lahko uporabi kot del svojih informacijskih operacij. Tovrstna tehnologija je lahko uporabljena proti zaveznicam za ustvarjanje napačnih novic, vplivanje na javne razprave, zmanjševanje zaupanja prebivalstva in kot poskus za izsiljevanje diplomatov.

V preteklosti so strokovnjaki ponaredke lahko razkrili, toda razvoj zelo napredne tehnologije prihaja do točke, na kateri bo kmalu lahko prevaral forenzična analitična orodja. Da bi se bili sposobni braniti pred tehnologijo, ki omogoča t. i. globoke prevare, v ZDA pod okriljem DARPA izvajajo projekt z naslovom »Media Forensics – MediFor«, katerega cilj je avtomatična detekcija manipulacij, ki zagotavlja podrobne informacije o tem, kako so bile manipulacije izvedene, in ugotavljanje integritete vizualnih medijev. Projekt je razvil nekatera začetna orodja, s katerimi lahko ugotovijo, kateri ponaredki so bili ustvarjeni s pomočjo UI. Težava je, da so lahko pametni stroji naučeni, da presežejo forenzična orodja, zato si v ZDA prizadevajo, da bi forenzična orodja razvijali z enako hitrostjo, kot se razvijajo tehnologije, ki omogočajo opisane prevare.

[4] *Izraz »heker« (hecker) se največkrat uporablja v zvezi z ljudmi, ki se ukvarjajo z vdori oziroma nepooblaščenimi dostopi v računalniška omrežja in z načini, kako obiti varnostne sisteme.*

Umetna inteligenca je lahko uporabljena tudi za ustvarjanje popolnih digitalnih vzorcev življenja, v katerih je na primer digitalni odtis določene osebe združen z njegovo zgodovino nakupovalnih navad, poročil o kreditni sposobnosti, profesionalnim življenjepisom in članstvi. Tako se ustvari določen vedenjski profil pripadnika oboroženih sil, obveščevalca, vladnega uslužbenca, diplomata ali navadnega državljana. Ta informacija je lahko, tako kot v primeru t. i. globokih prevar, uporabljena za vplivanje na določeno osebo ali njeno izsiljevanje (Rempfer, 2018).

4.5 Poveljevanje in kontrola

Ameriška vojska si prizadeva, da bi izkoristila potencial, ki ga ima UI tudi na področju poveljevanja in kontrole.

Letalstvo razvija sistem Večdimenzionalnega poveljevanja in kontrole (Multi-domain Command and Control – MDC2), s katerim namerava centralizirati načrtovanje in izvedbo operacij v zraku, vesolju, kibernetskem prostoru, na morju in kopnem. V neposredni prihodnosti bo umetna inteligenca uporabljena za združevanje podatkov iz senzorjev v vseh domenah vojskovanja. Oblikovan bo en vir informacij oziroma skupna operativna slika (common operational picture) določene situacije ali operacije, ki jo bodo videli odločevalci (Pomerlau, 2016). Danes informacije do odločevalcev prihajajo iz različnih platform v različnih formatih, pogosto se podvajajo ali pa med seboj pomembno razlikujejo. Skupna operativna slika, ki bo temeljila na umetni inteligenci, naj bi (vsaj teoretično) združevala vse različne informacije v eno sliko, pred tem pa naj bi UI avtomatično rešila dosedanje težave, ki jih imamo z vnesenimi podatki. Sistem MDC2 je trenutno v fazi razvoja koncepta, pri čemer ameriško letalstvo sodeluje s podjetjema Lockhead Martin in Harris ter nekaterimi start-up podjetji (Reynolds, 2018). Leta 2018 je bilo izvedenih tudi nekaj vojnih iger, s katerimi so poskušali določiti zahteve za razvoj koncepta.

Podobno DARPA razvija program z naslovom Mosaic Warfare Program, ki naj bi pomagal pri koordinaciji med avtonomnimi silami in dinamično generiranimi večdomenskimi vozlišči (node) poveljevanja in kontrole. Prihodnji sistemi UI bodo uporabljani za prepoznavanje prekinitev v komunikacijskih povezavah, ki jih je povzročil sovražnik, in sposobni poiskati nove, alternativne možnosti za distribucijo informacij. Naprednejši sistemi UI bodo poveljnikom morda celo zagotovili izbor različnih smeri delovanja na podlagi analiz bojišča, ki bodo izvedene v realnem času, in s tem hitrejše prilagajanje na zapletene dogodke. Mnogi analitiki verjamejo, da bi bil razvoj umetne inteligence na tem področju še posebej pomemben, saj bi lahko pospešil in izboljšal proces odločanja v vojni.

4.6 Polavtonomna in avtonomna vozila

Vse zvrsti ameriške vojske že delujejo v smeri združevanja umetne inteligence v polavtonomna in avtonomna vozila, vključno z bojnimi letali, droni, kopenskimi vozili in vodnimi plovili (DoD, 2017). Aplikacije UI na tem področju so podobne

tistim, ki se uporabljajo pri razvoju komercialnih vozil. Vozila, ki uporabljajo UI, zaznavajo okolje, prepoznavajo ovire, združujejo podatke s senzorjev, načrtujejo pot in celo komunicirajo z drugimi vozili.

Raziskovalni laboratorij ameriškega letalstva je končal drugo fazo preskusov programa Loyal Wingman. Program je združil letalo brez posadke starejše generacije F-16 z letalom F-22 ali F-35, v katerih je posadka. F-16 platforma brez posadke je avtonomno reagirala na dogodke, ki niso bili programirani, kot so vreme in nepredvidene ovire. V nadaljevanju se pričakuje, da bo UI letalu brez posadke omogočila izvedbo nalog ter bo letalu s posadko pomagala izvesti naloge, kot je na primer motenje elektronskih groženj ali nošenje dodatnega orožja (Axe, 2017).

Kopenska vojska in marinci preizkušajo prototipe vozil, ki sledijo vojake ali vozila na bojišču in izvajajo neodvisne naloge. Večnamensko taktično transportno vozilo (Multi-Utility Tactical Transport – MUTT), ki ga preskušajo marinci, je vozilo, ki zmore prevažati stotine kilogramov dodatne opreme. Čeprav sistem v svoji trenutni konfiguraciji še ni avtonomen, naj bi v prihodnje bil bolj neodvisen. Kopenska vojska načrtuje uvedbo bojnega robotskega vozila (Robotic Combat Vehicle – RCV) z različnimi stopnjami avtonomnosti, vključno z navigacijo, opazovanjem in odstranjevanjem neeksplodiranih ubojnih sredstev. Ti sistemi bodo uporabljani skupaj z vozili, v katerih bo posadka, oziroma v vozilih, ki bodo lahko delovala s posadko ali brez nje (optionaly inhabited), v tako imenovanih kopenskih vozilih naslednje generacije (Next Generation Ground Vehicle) (CRS, 2018a in 2018b). Ta vozila naj bi bila vojakom predana v terensko testiranje že konec letošnjega leta.

DARPA je leta 2019 končala testiranje prototipa plovila brez posadke za kontinuirano zasledovanje v protipodmorniškem vojskovanju (Anti-Submarine Warfare Continuous Trail Unmanned Vessel), ki so ga poimenovali Morski lovec (Sea Hunter). Program je trenutno v pisarni za pomorske raziskave (Office of Naval research). Če bo Morski lovec uveden v uporabo, bo ameriški mornarici omogočil avtonomno navigacijo na odprtem morju, zamenjavo modularne nosilnosti in koordinacijo med nalogami z drugimi plovili brez posadke. Hkrati pa bo zagotavljal kontinuiran lov na podmornice v daljših časovnih razdobjih. Nekateri analisti trdijo, da bodo operativni stroški Morskega lovca okoli 20.000 ameriških dolarjev na dan, kar je v primerjavi s tradicionalnim rušilcem, ki stane 700.000 ameriških dolarjev na dan, občuten prihranek.

Obrambno ministrstvo preizkuša tudi zmogljivosti, podprte z UI, ki bi bile sposobne sodelovanja oziroma t. i. rojenja (swarming). Rojenje je poseben element pri razvoju avtonomnih vozil, pri čemer koncepti predvidevajo združevanje večjih formacij nizkocenovnih vozil, katerih namen je preobremenitev (owerwhelm) obrambnih sistemov manjših enot z vozili, ki sodelujejo pri izvajanju elektronskih napadov. Trenutno se na tem področju razvijajo različne zmogljivosti. Leta 2016 je na primer ameriška mornarica testirala roj petih čolnov brez posadke, ki so patruljirali na štirikrat štiri milje velikem območju, njihovo delovanje pa je bilo podprto z UI.

Njihova naloga je bila prestrezanje plovil »vsiljivcev«. Tovrstni eksperimenti bodo v prihodnje podlaga za razvoj nove tehnologije UI, ki bodo zagotavljale obrambo pristanišč, lov na podmornice in izvidovanje za odkrivanje formacij, ki jih sestavljajo večje ladje. Načrtujejo se tudi testiranja večjih rojev podvodnih dronov (DARPA, 2018).

4.7 Ubojni avtonomni oborožitveni sistemi

Ubojni avtonomni oborožitveni sistemi (Lethal Autonomous Weapon Systems – LAWS) so poseben razred oborožitvenih sistemov, ki za samostojno, od človekove kontrole neodvisno identifikacijo cilja in uporabo oborožitvenega sistema, ki bo deloval na cilj, uporabljajo senzorje in računalniške algoritme. Ti sistemi zaenkrat še ne obstajajo. Omogočili naj bi izvajanje vojaških operacij na območjih, kjer so komunikacije izjemno slabe ali jih ni in v katerih tradicionalni vojaški sistemi ne bi bili sposobni delovati. Na mednarodni ravni že potekajo razprave o pravnem, etičnem in strateškem vidiku uporabe teh orožij (CRS, 2019).

Ameriška vojska trdi, da tovrstnih sistemov v njihovem arzenalu še ni. Prav tako zagovarjajo, da ni pravnih omejitev za razvoj tovrstnih oborožitvenih sistemov. Direktiva obrambnega ministrstva št. 3000.09 »Avtonomija in oborožitveni sistemi« (DoD, 2017) predstavlja namero ministrstva na področju razvoja polavtonomnih in avtonomnih oborožitvenih sistemov.[5] Dokument zahteva, da so vsi sistemi, ne glede na klasifikacijo, oblikovani tako, da poveljnikom in operaterjem omogočajo ustrezno raven presoje nad uporabo sile. Kakršne koli spremembe na sistemih morajo skozi ustrezen proces, v katerem se presoja, ali sistem še izpolnjuje zahteve in sposobnost za delovanje, za katerega je bil oblikovan. Prav tako direktiva predpisuje, da morata biti razvoj in predaja vsakega avtonomnega in omejenega števila polavtonomnih orožij v operativno uporabo predhodno odobrena na ravni namestnika ministra za politiko, načelnika Združenega štaba oboroženih sil oziroma namestnika ministra za obrambo za nabave in vzdrževanje ali namestnika ministra za raziskave in inženiring. Iz opisanega nadzora najvišje ravni so izvzeti: avtonomna orožja, ki jih nadzirajo ljudje in se uporabljajo za točkovno obrambo platform ali objektov, v katerih so človeške posadke, pri tem pa se ne uporabljajo na človeške cilje, in avtonomna orožja, ki izvajajo neubojno, nekinetično silo, kot so na primer nekatere vrste elektronskega napada na materialne tarče.

Mnogi strokovnjaki in tudi vojaki danes izpostavljajo pomisleke proti uporabi avtonomnih oborožitvenih sistemov (Sharre, 2017). Toda zahodne vojske se bomo znašle pred dilemo, ki jo postavlja razvoj tovrstnih tehnologij v rokah potencialnih sovražnikov. Kitajski proizvajalci vojaške opreme že prodajajo drone, ki so po njihovih zagotovilih sposobni popolne avtonomije, vključno z izvedbo napada na tarčo z ubojnim učinkom.

[5] *ZDA so ena izmed 42 držav, ki so sprejele načela za razvoj umetne inteligence OECD (OECD Principles on AI).*

5 PRILOŽNOSTI IN IZZIVI, KI JIH PREDSTAVLJA UMETNA INTELIGENCA V KONTEKSTU NACIONALNE VARNOSTI

Umetna inteligenca v kontekstu nacionalne varnosti predstavlja vrsto posebnih priložnosti in izzivov. Njen vpliv bo odvisen od tega, kako pomembne bodo za odločevalce prednosti, ki jih prinaša, v primerjavi z možnostmi, da se omejijo ali celo odpravijo njene pomanjkljivosti.

Avtonomnost oziroma sposobnost samostojnega delovanja je prednost, ki jo zagotavlja UI. Avtonomni sistemi bodo sposobni dopolnjevati ali nadomestiti ljudi pri opravljanju različnih nalog, še posebej pri bolj zapletenih in kognitivno zahtevnih nalogah. Na splošno naj bi vojske s tovrstnimi sistemi veliko pridobile, še posebej tam, kjer bi ti sistemi nadomestili vojake, ki opravljajo enolične, nevarne ali umazane, zdravju škodljive naloge. V vojski bi to bili sistemi, ki bi nadomestili dolgotrajno zbiranje in analizo obveščevalnih podatkov, čiščenje kemično kontaminiranih okolij, iskanje in odstranjevanje improviziranih eksplozivnih sredstev. V teh vlogah lahko avtonomni sistemi zmanjšajo tveganja za poškodbe in žrtve med vojaki in zmanjšajo stroške delovanja. Mnogi strokovnjaki danes zagovarjajo, da gre za taktično in strateško potrebo ter za moralno obveznost, da razvijemo tovrstne sisteme (DoD DSB, 2016).

Hitrost je naslednja prednost, ki jo zagotavlja UI. Ta omogoča nekaterim sistemom izjemno hitro delovanje. Reagirajo lahko v gigaherčni hitrosti, kar omogoča pospešitev celotnega tempa bojevanja. Nekateri strokovnjaki opozarjajo, da bi bistveno večje hitrosti tempa bojevanja lahko imele negativen učinek, še posebej, če bi presegle človekovo sposobnost, da presoja in kontrolira potek dogodkov (Ryan, 2017 in Scharre, 2016, str. 23–24). Kljub tveganju naj bi ti sistemi zagotavljali izjemno prednost pri vojskovanju.

UI zagotavlja tudi vztrajnost, še posebej pri izvajanju dolgotrajnih nalog, ki presegajo to človekovo sposobnost. Sistemi UI naj bi tako zagotovili zbiranje obveščevalnih podatkov iz obsežnejših področij in skozi daljše časovno obdobje ter avtonomno odkrivanje odstopanj in kategorizacijo vedenja.

Če bodo sistemi UI izboljšali človeške zmogljivosti in zagotovili manj drage vojaške sisteme, ki bodo hkrati tudi zmogljivejši, UI lahko postane mnogokratnik vojaških učinkov. Majhen, poceni dron je lahko neučinkovit proti visoko razvitim sistemom, kot je letalo F-35, toda roj takšnih dronov bi potencialno lahko preobremenil celo visoko razvit tehnološki sistem. Posledično to pomeni velikanski prihranek denarja in morda celo opustitev nekaterih oborožitvenih platform (Ryan, 2017).

Sistemi UI bi lahko dvignili produktivnost, saj lahko prevzamejo nekatere rutinske naloge ali omogočijo taktike, kot je rojenje, ki zahteva minimalno človekovo sodelovanje (Arklin, 2017, str. 36).

Nekateri strokovnjaki opozarjajo, da bi širjenje sistemov UI lahko povzročilo, da vojaška moč ne bi bila več odvisna od številčnosti prebivalstva in ekonomske moči države. To bi lahko manjšim državam in nedržavnim akterjem omogočilo neuravnoteženo velik vpliv na vojskovališču, še posebej, če bi jim uspelo UI uporabiti za povečevanje bojnih učinkov (Allen and Chan, 2017, str. 23).

UI naj bi zagotovila prevlado na področju informacij (information superiority). Ameriška vojska ima danes okoli 11.000 dronov, s katerimi vsak dan izvajajo visokokakovostno snemanje. Kljub temu pa nima zadosti osebja ali sistema, ki bi te posnetke pregledoval in izluščil uporabno obveščevalno analizo. Ta problem se bo z nadaljevanjem zbiranja podatkov v prihodnje samo še povečeval (Harper, 2018).

Do letošnjega leta naj bi vsak človek na svetu proizvedel 1,7 megabita informacij vsako sekundo, kar pomeni, da se bo svetovni zbir podatkov povečal s 4,4 zetabita na skoraj 44 zetabitov (Marr, 2015).[6] Obveščevalni sistemi, podprti z UI, naj bi omogočali integracijo in pregledovanje velikih količin podatkov iz različnih virov in geografskih lokacij. Pri tem naj bi prepoznavali vzorce in koristne informacije in tako bistveno izboljšali obveščevalno analizo. Algoritmi UI naj bi proizvedli svoje lastne podatke za nadaljnje analize, pri čemer naj bi pretvorili nestrukturirane informacije na primer iz volišč, finančne podatke in rezultate volitev v pisno poročilo. Tovrstna orodja UI lahko izboljšajo kakovost informacij, ki so v konfliktu, na voljo odločevalcem (Allen in Chan, 2017, str. 32, 36).

Sistemi UI lahko proizvedejo nekonvencionalne, nepričakovane rezultate, ki lahko v vojaškem kontekstu pomenijo prednost v boju, še posebej, če bodo presenečenje za sovražnika. Toda sistemi UI lahko tudi zatajijo na nepričakovane načine. Strokovnjaki tako vedenje ocenjujejo kot krhkost in neprožnost sistemov. Opozarjajo, da bi lahko sistemi UI v nekem okolju delovali z drugačnimi predpostavkami kot ljudje, ti pa ne bodo mogli ugotoviti, kdaj je sistem zunaj omejitev, ki jih je predvidelo njihovo izvirno oblikovanje.

Sistemi UI imajo lahko tudi t. i. algoritmični predsodek (algorithmic bias), ki izhaja iz njihovega učenja. Raziskovalci so na primer opazili, da ima UI pri prepoznavanju obrazov rasni predsodek, ki izhaja iz pomanjkanja raznovrstnosti podob, na podlagi katerih se je sistem učil. Neki drugi sistem za procesiranje jezika je razvil predsodek spola (Barrett, 2018 in Knight, 2016). Ti predsodki, ki bi bili integrirani v sistem, a jih ne bi odkrili, bi lahko imeli v vojaškem kontekstu hude posledice.

Za vojsko predstavlja izziv tudi sposobnost sistemov UI, da se prilagodijo določenemu področju ali okolju (domain adaptability) oziroma različnim področjem ali okoljem. Neki sistem, ki je bil razvit, da prepozna in razume spletno besedilo, se je predvsem učil iz besedil, ki so pisana v formalnem jeziku, kot so na primer besedila na Wikipediji. Zato je bil ta sistem nesposoben interpretirati bolj neformalen jezik

[6] *En zetabit je en trilijon gigabitov.*

Twitterja. Tako bi se lahko zgodilo, da bi UI-sistemi nepravilno delovali, če so bili razviti za civilno okolje in prestavljeni v vojaškega.

Poseben izziv naj bi pomenile napake sistemov UI, ki bi bili uporabljeni v večjem številu. Ljudje nismo nezmotljivi, toda napake so navadno narejene na individualni ravni in niso vedno enake. Sistemi UI pa bi lahko napačno delovali simultano in na enak način, kar bi lahko povzročilo obsežne in destruktivne učinke.

Nepričakovane rezultate lahko povzroči tudi interakcija naših in sovražnikovih sistemov UI, ki so se učili iz drugačnih podatkov, z drugačnimi parametri in predsodki.

Pomembno tveganje pomeni tudi nezmožnost, da pojasnimo (explainability), kako najbolj sposobni algoritmi UI v resnici izvajajo procese in pridejo do rešitev. DARPA trenutno izvaja petletno raziskavo, s katero naj bi oblikovali algoritme, ki jih bo mogoče pojasniti. Tudi druge raziskovalne organizacije izvajajo t. i. povratne analize, s katerimi želijo bolje razumeti notranje procese UI. Nezmožnost pojasnjevanja je v vojaškem kontekstu lahko tvegana. Operater ima lahko preveč ali premalo zaupanja v sistem in oboje je lahko pri delovanju ali pri podajanju strokovne ocene tvegano. Strokovnjaki ocenjujejo, da imamo ljudje odklonilen odnos do odločitev, ki bi bile popolnoma odvisne od analize, ki temelji na UI, še posebej, če ne razumemo, kako je stroj do rešitve prišel. Ameriška študija pravi, da bo le večja možnost pojasnjevanja omogočila več zaupanja do sistemov UI (MITRE, 2017).

Hitenje na področju tehnologije je torej lahko nevarno, še posebej, če prej ne bomo celovito razumeli vseh mogočih nevarnosti, ki jih predstavlja tehnologija UI. Pri uvajanju sistemov UI ne smemo spregledati, da neki sistem individualno predstavlja majhno tveganje, združeni pa pomenijo kolektivno tveganje zaradi interakcije, do katere prihaja med sistemi.

Sklep

Umetna inteligenca ponuja vrsto priložnosti za uporabo, ki bodo vplivale tudi na nacionalno varnost. UI bo imela pomemben vpliv na razvoj vojaških zmogljivosti, a tudi na druga področja, ki so pomembna za varnost: energetika, informacije, kmetijstvo, proizvodnja materialov, finančni trgi, transport in razvoj biomedicine, pri čemer se metode UI uporabljajo že precej časa.

Ko govorimo o vojaških zmogljivostih so področja, na katerih se UI že uveljavlja oziroma bo v prihodnosti prisotna, različna. UI bo vgrajena v vojaške platforme. Na področju kibernetike podpira avtomatsko zaščito omrežij, računalnikov, programov in podatkov. UI na področju logistike zmanjšuje uporabo človeške delovne sile, omogoča prepoznavanje okvar, napoved potrebnih popravil in podobno. Pri prepoznavanju vojaških ciljev bo UI v pomoč pri razumevanju območja delovanja. Analizirala bo podatke, ki bodo zagotovili boljše prepoznavanje in natančnejše določanje položaja tarče. UI bo omogočila medicinske operacije na daljavo, podprla bo diagnosticiranje in evakuacijo. UI že podpira vojaške simulacije in usposabljanje. Danes in v

prihodnje se nakazujejo številne možnosti za njeno uporabo na področju urjenja, kar bo zmanjšalo stroške in povečalo varnost vojakov. UI bo vse bolj uporabljana v sistemih opazovanja, izvidovanja in nadzora, kar bo izboljšalo situacijsko zavedanje. UI omogoča hitro in učinkovito procesiranje številnih podatkov, kar lahko podpre proces odločanja. Algoritmi UI bodo vozilom in plovilom brez posadk ter dronom omogočali avtonomno premikanje in letenje, v prihodnosti pa tudi bojno delovanje.

Razvoj UI pomeni številne prednosti, pa tudi tveganja. Zato ponavljamo to, kar smo zapisali v uvod prispevka. V kontekstu nacionalne varnosti in še posebej pri uvajanju sistemov UI v vojsko je treba zagotoviti, da so odločevalci s tehnologijo seznanjeni, predvsem pa, da celovito razumejo morebitne učinke njene uporabe.

V posameznih državah, ki se ukvarjajo z razvojem tehnologij in oblikovanjem disciplin, povezanih z umetno inteligenco, že potekajo razprave o tem, kako zagotoviti, da bosta razvoj pametnih strojev in njihovo vedenje postavljena v prave moralne, etične, politične in pravne okvire. Na tem področju so dejavne tudi mednarodne organizacije, kot so Združeni Narodi, EU in OECD. Za demokratične države je oblikovanje teh okvirov zelo pomembno. Tema zahteva podrobno analizo in povsem ločen prispevek.

Umetna inteligenca je že bila vključena v vojaške operacije v Iraku in Siriji (sistem Maven). Tehnologije UI pomenijo tudi posebne izzive na področju vojaške integracije, še posebej, ker se večina UI razvija v zasebnem sektorju. To na področju razvoja tehnologij ni nič posebnega, toda primer ZDA kaže, da mora skoraj vsaka tehnologija UI skozi poseben proces in modifikacije, preden bo lahko uporabljena v vojaške namene. Spoprijeli se bomo tudi s kulturnimi izzivi. V ZDA nekatera podjetja ne želijo sodelovati z obrambnim ministrstvom zaradi etičnih pomislekov. Mnogo pomislekov pa je tudi na obrambnem ministrstvu, še posebej do avtonomnih orožij.

Na področju razvoja UI sta aktivni tudi Kitajska in Rusija. Kitajska po dosegljivih podatkih razvija predvsem UI, ki bi pomagala pri pridobivanju kakovostnejših informacij, ki bi izboljšale in pohitrile proces odločanja, ter razvija različna avtonomna vozila. Rusija pa naj bi se osredotočala na robotiko.

Kako bo razvoj umetne inteligence vplival na uporabo vojaškega instrumenta moči, ne moremo zanesljivo napovedati. Uporaba UI v vojaškem kontekstu ima številne prednosti. Tehnologija lahko zagotovi avtonomne operacije, izboljša proces vojaškega odločanja in poveča hitrost in obseg vojaških aktivnosti, UI pa predstavlja tudi številne izzive. Lahko je nepredvidljiva in ranljiva, z njo je mogoče manipulirati.

Strokovnjaki glede tega, kako pomembna bo UI v prihodnjih oboroženih spopadih, niso enotni. Nekateri menijo, da bo tehnologija UI imela manjši vpliv, drugi pa, da bo imela evolucijski, če že ne revolucionarni učinek. Ocenjujemo, da bodo pri

uporabi vojaškega instrumenta moči v prihodnje hitrost pri prepoznavanju groženj, krajši proces odločanja, natančnost in učinkovitost bojnega delovanja odločilni.

Tehnološki napredek naj bi pri razvoju vojaškega instrumenta moči največ prinesel velikim državam, ki razvoju zapletenih tehnologij in vojaškim zmogljivostim namenjajo veliko finančnih sredstev. A kot smo v preteklosti videli, razvoj skoraj vsake tehnologije sčasoma zahteva manjše finančne vložke. S padanjem cene bodo te tehnologije postale na voljo tudi manjšim državam in nedržavnim akterjem.

DAESH je v svojih operacijah že uporabljal drone, zato lahko v prihodnje pričakujemo, da bodo tudi teroristične skupine uporabljale avtonomna vozila, verjetna pa je tudi uporaba robotov za izvajanje atentatov. Natančna streliva so danes v lasti le visoko razvitih vojsk, v prihodnje bodo morda na bojišču delovala s pomočjo dronov. Droni bodo uporabljeni kot sredstvo za izvidovanje, opazovanje in dostavo eksploziva na večjih razdaljah.

Razvoj robotike in avtomatizacija bosta zelo verjetno povečali absolutno vojaško moč različnih akterjev in tako zmanjšali relativno vojaško moč velikih držav. Na dolgi rok bodo dovolj sposobne robotske zmogljivosti preoblikovale instrument vojaške moči in načine vojskovanja.

Literatura

1. *ACTUV Sea Hunter' Prototype Transitions to Office of Naval Research for Further Development, January 30, 2018, DARPA, https://www.darpa.mil/news-events/2018-01-30a.*
2. *Allen, G., Chan, T., 2017. Artificial Intelligence and National Security, Belfer Center for Science and International Affairs, July 2017, https://www.belfercenter.org/publication/artificial-intelligence-and-national-security.*
3. *Arklin, R. C., 2017. A Roboticist's Perspective on Lethal Autonomous Weapons Systems, v Perspectives on Lethal Autonomous Weapon Systems, United Nations Office for Disarmament Affairs, Occasional Papers, No. 30, November 2017, https://www.un-ilibrary.org/disarmament/unoda-occasional-papers-no-30-november-2017_7748aa31-en.*
4. *Artificial Inteligence Index: 2019 Annual Report, www.hai.stanford.eu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf.*
5. *Axe, D., 2017. US Air Force Sends Robotic F-16s into Mock Combat, The National Interest, May 16, 2017, http://nationalinterest.org/blog/the-buzz/us-air-force-sends-robotic-f-16s-mock-combat-20684.*
6. *Barrett, B., 2018. Lawmakers Can't Ignore Facial Recognition's Bias Anymore, Wired, July 26, 2018, https://www.wired.com/story/amazon-facial-recognition-congress-bias-law-enforcement.*
7. *Buchanan, B., Miller, T., 2017. Machine Learning for Policymakers: What It Is and Why It Matters, Belfer Center, www.belfercenter.org/publication/machine-learning-policymakers.*
8. *Corrigan, J., 2017. Tree star general wants AI in Every New Weapon System, Defense One, November 3, 2017, https://www.defenseone.com/technology/2017/11/three-star-general-wants-artificial-intelligence-every-new-weapon-system/142239/.*
9. *Directive 3000.09, 2017, Autonomy in Weapon Systems, DoD (US), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODd/300009p.pdf*

10. *Generating Actionable Understanding of Real-World Phenomena with AI January 4, 2019, DARPA, https://www.darpa.mil/news-events/2019-01-04.*
11. *Harper, J., 2018. Artificial Intelligence to Sort through ISR Data Glut, National Defense, January 16, 2018, http://www.nationaldefensemagazine.org/articles/2018/1/16/artificial-intelligence-to--sort-through-isr-data-glut.*
12. *Hiršman, M., 2014. Vloga umetne inteligence pri reševanju sodobnih izzivov ravanja s podatki, 2014, http://www.cek.ef.uni-lj.si/magister/hirsman1422-B.pdf*
13. *Issues in Autonomous Vehicle Deployment, 2018a CRS Report R44940, https://crsreports.congress.gov/product/pdf/R/R44940.*
14. *International Discussions Concerning Lethal Autonomous Weapon Systems, 2019, CRS Report, https://assets.documentcloud.org/documents/6305453/International-Discussions-Concerning-Lethal.pdf.*
15. *Knight, W., 2016. How to Fix Silicon Valley's Sexist Algorithms, MIT Technology Review, November 23, 2016, https://www.technologyreview.com/s/602950/how-to-fix-silicon-valleys-sexist-algorithms.*
16. *Li, S., 2019. Anomaly Detection for Dummies: Supervised Anomaly Detection for for Univariate & Multivariate Data, v Towards Data Science, 2019, www.towardsdatascience.com/anomaly-detection-for-dummies-15f148e559c1.*
17. *Lopez, C. T., 2019. DOD Expects Significant Progress on Critical F-35 System, November 2019, https://www.defense.gov/Explore/News/Article/Article/2016024/dod-expects-significant-progress-on-critical-f-35-system/.*
18. *Marr, B., 2015. Big Data: 20 Mind-Boggling Facts Everyone Must Read, Forbes, September 30, 2015, https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/ #539121d317b1.*
19. *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DOD, Office of the Assistant Secretary of Defense for Research and Engineering, January 2017, The MITRECorporation, https://fas.org/irp/agency/dod/jason/ai-dod.pdf.*
20. *Principles on AI, June 2019, OECD, https://www.oecd.org/going-digital/ai/principles.*
21. *Pomerlau, M., 2016. Loyal Wingman Program Seeks to Realize Benefits of Advancements in Autonomy, October 19, 2016, https://www.c4isrnet.com/unmanned/uas/2016/10/19/loyal-wingman-program-seeks-to-realize-benefits-ofadvancements-in-autonomy.*
22. *Pomerlau, M., 2017. How Industry's Helping the US Air Force with Multi-Domain Command and Control, Defense News, September 25, 2017, https://www.defensenews.com/c2-comms/2017/09/25/industry-pitches-in-to-help-air-forcewith-multi-domain-command-and-control/.*
23. *Poročilo o tekmovanju Grand Challenge, 2016, DARPA, https://www.darpa.mil/news-events/2016-08-04.*
24. *Rempfer, K., 2019. Ever heard of 'deep fake' technology? The phony audio and video tech could be used to blackmail US troops, Military Times, July 19, 2018, https://www.militarytimes.com/news/your-air-force/2018/07/19/ever-heard-of-deep-fake-technology-the-phony-audio-and-video-tech-could-be-used-to-blackmail-us-troops/.*
25. *Reynolds, J., 2018. Multi-Domain Command and Control is comming, US AIR Force, 25. September 2018, https://www.af.mil/News/Article-Display/Article/1644543/multi-domain-command-and-control-is-coming/.*
26. *Ryan, M., 2017. Building a Future: Integrating Human-Machine Military Organization, The Strategy Bridge, December 11, 2017, https://thestrategybridge.org/the-bridge/2017/12/11/building-a-future-integrated-human-machine-military-organization.*
27. *Rosenberg, S., 2017. Firewalls Don't Stop Hackers, AI Might, Wired, August 27, 2017, https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/*

28. *Scharre, P., 2016 Autonomous Weapons and Operational Risk, Center for a New American Security, February 2016, https://www.files.ethz.ch/isn/196288/CNAS_Autonomous-weapons-operational-risk.pdf.*
29. *Scharre, P., 2017. A Security Perspective: Security Concerns and Possible Arms Control Approaches«, v Perspectives on Lethal Autonomous Weapon Systems, United Nations Office for Disarmament Affairs, Occasional Papers, No. 30, November 2017, https://www.un-ilibrary.org/disarmament/unoda-occasional-papers-no-30-november-2017_6b5db3ba-en.*
30. *Stone, A., 2017. Army Logistics Integrating New AI, Cloud Capabilities«, September 7, 2017, https://www.c4isrnet.com/home/2017/09/07/army-logistics-integrating-new-ai-cloud-capabilities/.*
31. *Summer Study on Autonomy, June 9, 2016, DoD (US) Defense Science Board (DSC), https://www.acq.osd.mil/dsb/reports/2010s/DSBSS15.pdf.*
32. *Svet Elektronike, »PULP Dronet: 27-gramski dron, ki so ga navdihnili insekti«, November 2019, https://www.svet-el.si/revija/novice/2019-279-08/.*
33. *U.S. Ground Forces Robotics and Autonom, 2018b, CRS Report R45392, https://digital.library.unt.edu/ark:/67531/metadc1442984/.*
34. *Weisgerber, M., 2017. The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS«, Defense One, May 14, 2017, http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-itsfirst-mission-hunt-isis/137833/.*