

DIPLOMSKI RAD

**PANEVROPSKI UNIVERZITET APEIRON
FAKULTET INFORMACIONIH TEHNOLOGIJA
Banjaluka**

**Vanredne studije
Studijski program: Poslovna informatika**

„VJEŠTAČKA INTELIGENCIJA U VOJSCI I SAVREMENI ASPEKTI NACIONALNE BEZBJEDNOST ”

**Mentor:
Prof. dr Branko Latinović**

**Student:
Darko Rogić**

Banjaluka, jul 2019.

PANEVROPSKI UNIVERZITET „APEIRON“
FAKULTET INFORMACIONIH TEHNOLOGIJA
BANJA LUKA

Darko Rogić

VJEŠTAČKA INTELIGENCIJA U VOJSCI I SAVREMENI
ASPEKTI NACIONALNE BEZBJEDNOST

Diplomski / Specijalistički rad

IZJAVA:

Ja, Darko Rogić, student Univerziteta Panevropski Univerzitet »Apeiron« Fakultet informacionih tehnologija Banja Luka, odgovorno i uz moralnu i akademsku odgovornost izjavljujem da sam ovaj diplomski rad izradio potpuno samostalno uz korištenje citirane literature i pomoć mentora.

Mentor: Prof. dr Branko Latinović

Student: Darko Rogić

Broj indeksa: 155-14/VPI

Banja Luka, jul, 2019. godine

SADRŽAJ

1. UVOD	4
2. VJEŠTAČKA INTELIGENCIJA	6
2.1. Istorijski razvoj vještačke inteligencije	6
2.2. Ciljevi vještačke inteligencije.....	7
2.3. Modelovanje vještačke inteligencije i ljudske performanse.....	9
3. SADAŠNJA I POTENCIJALNA UPOTREBA VJEŠTAČKE INTELIGENCIJE U VOJSCI	11
3.1. Vještačka inteligencija i aplikacije vezane za odbranu	11
3.1.1. Inteligencija, nadzor i izviđanje	12
3.1.2. Logistika	13
3.1.3. Cyberspace operacije	14
3.1.4. Informacione operacije i „Deep Fakes“	14
3.1.5. Komanda i kontrola.....	15
3.1.6. Poluautonomna i autonomna vozila.....	16
3.2. Smrtonosni autonomni sistemi oružja	19
3.3. Izazovi integracije vojne vještačke inteligencije	20
3.3.1. Tehnologija	21
3.3.2. Proces i postupci	21
3.3.3. Osoblje	22
3.3.4. Kultura	23
3.4. Mogućnosti i izazovi vještačke inteligencije u vojsci	24
3.4.1. Autonomija	25
3.4.2. Brzina i izdržljivost.....	26
3.4.3. Skaliranje	26
3.4.4. Superiornost informacija.....	27
3.4.5. Predvidljivost	28
3.4.6. Eksploatacija.....	32
3.5. Autonomna oružja i vojska.....	33
3.5.1. Tehnički izazovi.....	35

3.5.2.	Definisanje autonomnog segmenta vještačke inteligencije	38
3.5.3.	Etička pitanja vještačke inteligencije u vojsci	39
3.5.4.	Prelaz na nova područja autonomije u vojsci	40
4.	ZAKLJUČAK	41
5.	LITERATURA	43

1. UVOD

Vještačka inteligencija (AI), se može definisati kao grana informatike koja se bavi automatizacijom inteligentnog ponašanja. Ova definicija posebno odgovara u pogledu naglašavanja uvjerenja da je AI dio računarske nauke i, kao takva, mora biti zasnovana na zdravim teorijskim i primjenjenim principima koji se zasnivaju na ovom polju informatike u domenima ekspertnih sistema.

Ovi principi uključuju strukture podataka koji se koriste u predstavljanju znanja, algoritama koji su potrebni za primjenu tog znanja, kao i njihovi jezici i tehnike programiranja, koje se koriste u njihovoj realizaciji. Međutim, ova definicija pati od činjenice da sama inteligencija nije dobro definisana ili čestno neadekvatno razumljiva. Iako većina nas sigurna da znamo o inteligentnom ponašanju kada ga vidimo, upitno je da svako može da dođe blizu definisanja podataka na način na koji će biti dovoljno specifična da pomognu u procjeni navodno inteligentnih kompjuterskih programa, u sverama kompleksnosti ljudskog uma.

Ekpertni sistemi su računarski programi koji su izvedeni iz grane istraživanja informatike, koja se i naziva vještačka inteligencija. Naučni cilj AI je da razumije inteligenciju, izgradnjom računarskih programa koji pokazuju inteligentan način ponašanja. Bavi se konceptima i metodama simboličkog zaključivanja, ili rasuđivanja, na računaru, a informatičko znanje se koristi da bi ti zaključci bili predstavljeni u mašini (robotika). Naravno, termin inteligencija obuhvata mnoge kognitivne sposobnosti, uključujući i sposobnost rješavanja problema, učenja, i razumijevanja informatičkog jezika. Najveći napredak do danas u AI je postignut u oblasti rješavanja problema - koncepata i metoda za izgradnju humanoidnih programa.

AI programi koji ostvaruju nadležnost stručnjaka u nivou informatičkog rješavanja problema u operativnim oblastima podrazumijevaju primjenu znanja o specifičnim vještačkim zadacima na bazi stručnosti ili znanja o ljudskom ponašanju. Često, ekspertske sistemi su termin koji je rezervisan za programe čije je znanje baza, koja sadrži znanje koje koristi ljudske stručnjake, za razliku od znanja prikupljenih iz udžbenika ili ne-stručnjaka (amatera). Izgradnja stručnog sistema je poznata kao inženjering znanja i njeni stručnjaci se nazivaju inženjeri znanja. Inženjer znanja mora biti siguran da računar ima svo znanje potrebno da riješi neki problem. Inženjer znanja mora izabrati jedan ili više oblika u kojima se predstavlja potrebno

znanje kao simbol obrazaca u memoriji računara - to jest, on mora izabrati predstavljanje znanja u svjetlu savremene informatike i ekspertnih sistema. On takođe mora osigurati da računar može efikasno koristiti znanje i to izborom od nekolicine metoda rezonovanja u informatičkom kontekstu (vještačka inteligencija).

2. VJEŠTAČKA INTELIGENCIJA

Vještačka inteligencija kao pojam u širem smislu, označava kapacitet jedne vještačke tvorevine za realizovanje funkcija koje su karakteristika ljudskog razmišljanja. Mogućnost razvoja slične tvorevine je budila interesovanje ljudi još od antičkog doba, ipak, tek u drugoj polovini XX vijeka takva mogućnost je dobila prva oruđa (računare), čime se otvorio put za taj poduhvat.¹ U kontekstu razvoja savremene nauke, istraživačke aktivnosti vještačke inteligencije su se kretale u dva pravca i to: tehnološki razvoj naprednih računarskih sistema i istraživanja koja se tiču fiziološke i psihološke prirode ljudskog razmišljanja odnosno uma.

Današnja, savremena istraživanja u oblasti vještačke inteligencije koncentrisana su na programska rješenja računarske informacije u svrhu konstruisanja inteligentnih mašina koje će imati inteligentne sposobnosti slične ljudima. Savremene tendencije u domenu vještačke inteligencije vezane su za razvoj neuronskih mreža i unapređivanje ekspertnih sistema. Uloga ekspertskih sistema u ovom kontekstu je reprodukcija ljudskog razmišljanja preko specifičnih simbola pretočenih u vještačku inteligenciju. Ako posmatramo neuronske mreže njihov koncept se posmatra sa aspekta biološke perspektive, a rezultati su još uvijek daleko od inteligentnog razmišljanja. Takođe, i dalje je prisutno razmišljanje da je trenutna situacija još daleko od inteligentnog. Savremena istraživanja su fokusirana na učenje, razmišljanje, rješavanje problema, percepciju i razumijevanje prirodnog jezika.²

2.1. Istorijski razvoj vještačke inteligencije

Ako posmatramo vještačku inteligenciju u istorijskom kontekstu potrebno je prvo poći od same definicije i njenog pojavljivanja. Definiciju vještačke inteligencije, odnosno pojam je prvi put predstavljen 1956. godine u Hanoveru u SAD, na simpozijumu istraživača koji su predstavljali teorije koje su vezane za inteligenciju, neuronske mreže i automate (robote). Ovaj simpozijum je organizovan od strane Džona Makartija i njegovih saradnika i na njemu su postavljeni temelji vještačke inteligencije, i otvoren put ka njenom daljem razvoju i

¹ Janičić, P., Nikolić, M. (2017), *Vještačka inteligencija*, Beograd: Matematički fakultet Univerziteta u Beogradu, str. 75.

² Ilić, V. (1999), *Vještačka inteligencija*, Beograd: SOLAIR, str. 27.

usavršavanju. Prije ovog sipozijuma, još 1950. godine, naučnik Alan Tjuring je u svom članku u reviji „Mind“ pisao o konceptima vještačke inteligencije i opisao vrstu probe koja je vezana za vještačku inteligenciju, koja je danas poznata kao „Tjuringov test“, prema kome se vrši procjena da li je neki sistem inteligentan ili ne.

Već spomenuti simpozijum je organizovan u svjetlu ranijih istraživanja i u kontekstu predstavljanja programa *Logic Theorist*, koji je u tom vremenu napravio senzaciju u domenu ekspernih sistema i vještačke inteligencije. Smatra se da je i taj program svojevrsna osnova za današnje tendencije razvoja u polju vještačke inteligencije. Iako se ova istraživanja smatraju začetkom vještačke inteligencije, postoje mnoga druga koji su bitno uticala na razvoj ove oblasti. Neka potiču iz oblasti kao što su filozofija (prvi pokušaji formalizacije rezonovanja su silogizmi grčkog filozofa Aristotela), matematika (teorija odlučivanja i teorija probabiliteta se primjenjuju u mnogim današnjim sistemima), ili psihologija (koja je zajedno sa vještačkom inteligencijom formirala oblast kognitivne nauke).³

U narednim godinama, koncept vještačke inteligencije se ubrzano usavršavao, a razvoj je danas u najvećem obimu, pa se istraživači širom svijeta utrkuju ko će napraviti najinteligentniju mašinu i da će vještačka inteligencija dostići imaginarnu granicu stvaranja robota koji će imati inteligenciju sličnu ili istu kao i čovjek („homo roboticus“).⁴

2.2. Ciljevi vještačke inteligencije

Smatra se da je cilj vještačke inteligencije konstruisanje informatičkog rješenja koje će imati osobine inteligentnog „bića“, odnosno mašine koja će imati inteligentne karakteristike. Svaka mašina u tom kontekstu mora imati ljudsko i vještačko inteligentno ponašanje. Da bi razumjeli vještačku inteligenciju potrebno je obrazložiti i koncept „Tjuringovog testa“, u kome je Alan Tjuring predložio eksperimentalno rješenje pomoću koga možemo izvršiti procjenu

³ Janičić, P., Nikolić, M. (2017), *Veštačka inteligencija*, Beograd: Matematički fakultet Univerziteta u Beogradu, str. 75.

⁴ Janičić, P., Nikolić, M. (2017), *Veštačka inteligencija*, Beograd: Matematički fakultet Univerziteta u Beogradu, str. 76.

inteligentnog ponašanja neke mašine.⁵ Ovaj test se zasniva na „pogađanju“ pola jednog od dva interlokutora, što je prikazano na slici 1.

Princip je takav da postoje dva interlokutora (A i B), koji se nalaze u odvojenim, posebnim sobama. Iako u principu oba tvrde da su ženskog pola, riječ je o muškarcu i ženi. U izvornom Tjuringovom prijedlogu urađena je izvjesna modifikacija, te je ženu zamijenio računar. Uloga ispitivača je da pogodi ko je od A i B mašina, a na osnovu međusobnog razgovora, imajući u vidu da je tvrdnja da je riječ o ljudima (ljudskim bićima). Zadatak se mora ostvariti i pored činjenice da nijedan od interlokutora nije dužan da govori istinu (ima mogućnost da ne govodi istinu – da laže). Aparat (mašina) ima mogućnost, odnosno može odlučiti da da pogrešan rezultat, a na osnovu rezultata aritmetičke operacije ili da ga saopšti nešto kasnije, da bi neistina bila što uvjerljivija.

Slika 1. Koncept Tjuringovog testa



Sam Tjuring je zastupao tezu da će još 2000. godine postojati računari koji će imati sposobnost da igraju ovu vrstu „igre“, tako da prosječan ispitivač nema više od 70% šanse da uradi ispravnu identifikaciju, nakon pet minuta postavljanja pitanja. Da je on bio u pravu, danas bi bili u mogućnosti da ispred sebe imamo mašinu koja je uistinu inteligentna, odnosno koja može da se predstavi kao inteligentna. Problem zbog koga to nije tako je zbog sposobnosti ili tačnije nesposobnosti računara za pravilnu obradu podataka, a ne u pogledu toga da stručnjaci

⁵ Ilić, V. (1999), *Veštačka inteligencija*, Beograd: SOLAIR, str. 28.

nisu u sposobnosti da konstruišu (programiraju) mašinu sa sposobnošću inteligentnog ponašanja.⁶

Ako posmatramo vještačku inteligenciju danas, možemo reći da je cilj postizanje dva komplementarna cilja, a to su teorijski i tehnološki aspekt. Ovi ciljevi su direktno vezani za istraživačke, a ne za kreatorske funkcije vještačke inteligencije (programiranje).

2.3. Modelovanje vještačke inteligencije i ljudske performanse

Mnogi AI programi su napravljeni da riješe neke korisne probleme bez obzira na njihove sličnosti sa ljudskom mentalnom arhitekturom. Čak i ekspertske sistemi, iako se u njihovom izvođenju koristi mnogo znanja stručnjaka, stvarno ne pokušavaju da simuliraju ljudsko unutrašnje rješavanje mentalnih procesa, sa aspekta rješavanja problema. Ako mentalna predstava predstavlja jedini kriterijum na kome će vještački sistem funkcionisati, onda možda postoji malo razloga da se pokušaju simulirati ljudske metode rješavanja problema; u stvari, programi koji kroz nehumane pristupe rješavaju probleme (primjer igre šaha, koju će računar skoro uvijek riješiti u svoju korist), pa računari često imaju više uspjeha nego njihove ljudske „kolege“.⁷

Ipak, dizajn sistema koji eksplicitno daje predstavu modela ljudske predstave, predstavlja plodno područje istraživanja u oblasti AI i psihologije. Vještačka inteligencija je u tom kontekstu postala moćan alat za formulisanje i testiranje teorije „*human cognition*“, odnosno ljudske kognicije.⁸ Metodologije rješavanja problema koje je razvio tim kompjuterskih naučnika, dali su psiholozima novu metaforu za istraživanje ljudskog uma u kontekstu razumijevanja vještačke inteligencije. Ne samo da su ove tehnike obezbjeđuju novi vokabular za opisivanje ljudske inteligencije, ali i kompjuterske implementacije ove teorije nude psiholozima priliku da kreiraju empirijski test, koji će pomoći kako ljudima, tako i stručnjacima za razvoj koncepta vještačke inteligencije.

⁶ Ilić, V. (1999), *Veštačka inteligencija*, Beograd: SOLAIR, str. 29.

⁷ Luger, G. (2007), *Artificial intelligence*, sixth edition, Boston: University of New Mexico, str. 25.

⁸ Luger, G. (2007), *Artificial intelligence*, sixth edition, Boston: University of New Mexico, str. 26.

Tipični sistem za treniranje učenika i studenata u kontekstu vještačke inteligencije se obično sastoji od četiri osnovne komponente.

- Prva komponenta je okruženje u kojem učenik ili student radi na rješavanju složenih zadataka. To može biti simulacija komponente ili komponenata elektronskih uređaja predstavljena kao serija problema koje student treba da riješi.
- Druga komponenta je ekspertski sistem koji može riješiti predstavljene probleme na kojima student radi.
- Treću čini jedan poseban modul koji može uporediti rješenja koja nudi student sa onima koje su ugrađene u ekspertski sistem i njegov cilj je da prepozna studentov plan za rješavanje problema, kao i koje dijelove znanja najvjerojatnije student koristi.
- Četvrtu čini pedagoški modul koji sugeriše zadatke koje treba riješiti, odgovara na pitanja studenta i ukazuje mu na moguće greške. Odgovori na pitanja studenta i sugestije za planiranje rješavanja zadataka, zasnivaju se na prikupljenim podacima iz prethodnog modula.

Svaka od ovih komponenata može koristiti tehnologiju vještačke inteligencije. Okruženje može sadržati sofisticiranu simulaciju ili inteligentnog agenta, odnosno simuliranog studenta ili čak oponenta studentu. Modul koji čini ekspertski sistem se sastoji od klasičnih problema vještačke inteligencije, kao što su prepoznavanje plana i rezonovanje nad problemima koji uključuju neizvjesnost.

3. SADAŠNJA I POTENCIJALNA UPOTREBA VJEŠTAČKE INTELIGENCIJE U VOJSCI

Vještačka inteligencija (AI) je brzo rastuća oblast tehnologije koja privlači pažnju komercijalnih investitora, intelektualaca iz domena odbrane, kreatora politika i međunarodnih konkurenata, o čemu svjedoče brojne nedavne inicijative. Kineska vlada je 20. jula 2017. objavila strategiju koja detaljno opisuje svoj plan da preuzme vodstvo u AI do 2030. godine. Manje od dva mjeseca kasnije Vladimir Putin je javno objavio namjeru Rusije da slijedi AI tehnologije, navodeći da će Rusija u ovoj oblasti vladati svijetom.⁹

Slično tome, Američka Nacionalna strategija odbrane, objavljena u januaru 2018. godine, identifikovala je vještačku inteligenciju kao jednu od ključnih tehnologija koja će osigurati Sjedinjenim Državama da se mogu boriti i pobijediti u ratovima. Američka vojska već integriše AI sisteme u borbu putem inicijative pod nazivom Project Maven, koja koristi AI algoritme za identifikaciju pobunjeničkih ciljeva u Iraku i Siriji. Koje vrste vojnih aplikacija AI su moguće, i koje granice, ako ih ima, treba nametnuti? Koje jedinstvene prednosti i slabosti dolaze sa uključivanjem AI u odbranu? Kako će AI promijeniti ratovanje i kakav će uticaj imati na vojnu ravnotežu? U SAD na primjer Kongres ima brojne nadzorne, budžetske i zakonodavne alate na raspolaganju da bi mogao uticati na odgovore na ova pitanja i oblikovati budući razvoj AI.¹⁰

3.1. Vještačka inteligencija i aplikacije vezane za odbranu

Različita ministarstva i sektori u svijetu u modernom vremenu razmatraju niz različitih aplikacija za AI. Trenutno je istraživanje i razvoj AI prepušteno diskreciji istraživačkih organizacija u pojedinačnim službama, kao npr. DARPA (*Defense Advanced Research Projects Agency*) i Agencija za napredne istraživačke projekte (IARPA) u SAD. JAIC je u SAD zadužen

⁹ Weisgerber, M. (2017), "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS", *Defense One*, May 14.

– <http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/>

¹⁰ Weisgerber, M. (2017), "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS", *Defense One*, May 14.

da nadgleda inicijative nacionalnih misija, projekte koji će uticati na AI za rješavanje hitnih operativnih izazova. Kancelarija podsekretara odbrane za istraživanje i inženjering u SAD, koja je nadgledala razvoj AI strategije Ministarstva odbrane. Cross-Functional Team Algoritamskog ratovanja, poznat i kao Project Maven, ranije je bio žarišna tačka za integraciju AI u SAD. Project Maven je pokrenut u aprilu 2017. i zadužen je za brzo uključivanje AI u postojeće DOD sisteme kako bi demonstrirao potencijal tehnologije. Inicijalni direktor projekta Maven izjavio je: “Maven je dizajniran da bude pilot projekat, taj putokaz, ta iskra koja pali plamen za vještačku inteligenciju preko odjeljenja i osigura nacionalnu bezbjednost u SAD”.¹¹ Sličan slučaj je u Kini, Rusiji, Indiji i Japanu, ali drugim „snažnijim“ državama svijeta. AI se takođe inkorporira u niz drugih obavještajnih, nadzornih i izviđačkih aplikacija, kao i u logistici, operacijama u sajber prostoru, informacionim operacijama, komandi i kontroli, polu-autonomnim i autonomnim vozilima i smrtonosnim autonomnim sistemima naoružanja.

3.1.1. Inteligencija, nadzor i izvidanje

Očekuje se da će AI biti posebno korisna za obavještajne podatke zbog velikih skupova podataka dostupnih za analizu. Na primjer, prva faza projekta Maven uključuje automatizaciju obrade obavještajnih podataka kao podršku protiv ISIL kampanje. Konkretno, Project Maven tim uključuje algoritme za kompjutersku viziju i računarsko učenje u inteligentne ćelije za prikupljanje koje bi češljale snimke iz nenaseljenih letilica i automatski identifikovane neprijateljske aktivnosti za ciljanje neprijateljskih lokacija širom svijeta. U tom svojstvu, AI ima za cilj da automatizuje rad ljudskih analitičara koji trenutno provode sate analizirajući video snimke za korisne informacije, potencijalno oslobađajući analitičare da donose efikasnije i pravovremene odluke na osnovu podataka iz AI sistema.¹²

Obavještajna zajednica u svijetu takođe ima veliki broj javno priznatih AI istraživačkih projekata, koji su u toku, a sigurno još toliko njih koji se sprovode u tajnosti. Sama Centralna obavještajna agencija (CIA) u SAD ima oko 140 projekata u razvoju koji koriste AI u određenom kapacitetu za izvršavanje zadataka kao što su prepoznavanje slika i prediktivna analitika. IARPA sponzoriše nekoliko AI istraživačkih projekata namijenjenih za proizvodnju

¹¹ McKinsey Global Institute (2017), Artificial Intelligence, The Next Digital Frontier?, p. 4-6.

¹² Koch, C. (2016), “How the Computer Beat the Go Master,” *Scientific American*, 19 March, str. 21.

drugih analitičkih alata u narednih četiri do pet godina. Neki primjeri uključuju razvoj algoritama za višejezično prepoznavanje i prevođenje govora u bučnim okruženjima, geolociranje slika bez pridruženih metapodataka, spajanje 2-D slika za kreiranje 3-D modela i izgradnju alata za zaključivanje funkcije zgrade na osnovu modela analiza života ljudi.¹³

3.1.2. Logistika

AI može imati perspektivnu budućnost u oblasti vojne logistike. Vazduhoplovstvo, na primjer, počinje da koristi AI za predviđanje održavanja aviona. Umjesto popravke kada se avion slomi ili u skladu sa monolitnim planovima održavanja flote, vazduhoplovstvo testira AI-pristup koji prilagođava rasporede održavanja potrebama pojedinačnih aviona. Ovaj pristup, koji se trenutno koristi u Automatizovanom logističkom informacionom sistemu F-35, izvlači podatke senzora u realnom vremenu ugrađene u motore aviona i druge sisteme na brodu i unosi podatke u algoritam predviđanja kako bi odredio kada tehničari trebaju pregledati avion ili zamijeniti dijelove.¹⁴

Slično tome, aktivnost Logističke podrške vojske SAD (LOGSA) ugovorila je korištenje IBM-ovog Watson-a (isti AI softver koji je porazio dva šampiona Jeopardy-a) kako bi razvio prilagođene rasporede održavanja za Striker-ovu flotu na osnovu informacija iz 17 senzora instaliranih na svakom vozilu. U septembru 2017. godine, LOGSA je započela drugi projekat koji će koristiti Watson za analizu tokova otpreme za distribuciju dijelova za popravke, pokušavajući odrediti najučinkovitiji način isporuke. Ovaj zadatak trenutno izvršavaju ljudski analitičari, koji su vojsku spasili troškova od oko 100 miliona dolara godišnje, analizirajući samo 10% zahtjeva za otpremu; sa Watson-om, vojska će imati sposobnost da analizira 100% zahtjeva za otpremu, što potencijalno može da generiše još veće uštede u kraćem vremenskom periodu.

¹³ Schmidhuber, J. (2014), "Deep Learning in Neural Networks: An Overview," *Technical Report IDSIA-03-14*, arXiv:1404.7828 v4.

¹⁴ Campbell, M. (2015), "Knowledge discovery in Deep Blue," *Comm. of the ACM* 42, Nov., str. 38.

3.1.3. Cyberspace operacije

AI će vjerovatno biti ključna tehnologija u unaprjeđivanju vojnih sajber operacija. U svom svjedočenju iz 2016. pred Komitetom oružanih snaga Senata, komandant američke Cyber komande admiral Majkl Rodžers izjavio je da je oslanjanje na ljudsku inteligenciju samo u sajber prostoru „strategija gubitka“.¹⁵

Konvencionalni alati za sajber bezbjednost traže istorijske podudarnosti sa poznatim zlonamjernim kodom, tako da hakeri samo moraju da modifikuju male dijelove tog koda da bi zaobišli odbranu. Alati sa omogućenom inteligentnom inteligencijom, s druge strane, mogu biti obučeni da detektuju anomalije u širem obrascu mrežne aktivnosti, te tako predstavljaju sveobuhvatniju i dinamičniju barijeru za napad.

DARPA 2016 Cyber Grand Challenge demonstrirao je potencijalnu moć alata za sajber alate. Takmičenje je izazvalo učesnike da razviju AI algoritme koji bi mogli autonomno da detektuju, procjenjuju i zakrpe ranjivosti softvera prije nego što takmičarski timovi imaju priliku da ih iskoriste - sve u roku od nekoliko sekundi, umjesto uobičajenih mjeseci, ne samo potencijalnu brzinu sajber alata sa omogućenom inteligentnom inteligencijom, već i potencijalnu mogućnost singularnog algoritma da istovremeno izvršava napad i odbranu. Ove sposobnosti bi mogle da pruže jasnu prednost u budućim sajber operacijama.

3.1.4. Informacione operacije i „Deep Fakes“

AI omogućava sve realističnije fotografije, audio i video falsifikate, ili „duboke krivotvorine“, koje bi protivnici mogli primijeniti kao dio svojih informacionih operacija. Zaista, duboka lažna tehnologija mogla bi se koristiti protiv saveznika Sjedinjenih Država i samih SAD-a za generisanje lažnih vijesti, uticanje na javni diskurs, narušavanje javnog povjerenja i pokušaj ucjenjivanja diplomata. Iako su većinu prethodnih dubokih krivotvorina otkrili stručnjaci, sofisticiranost tehnologija napreduje do tačke da će uskoro biti u stanju da zavara forenzičke analitičke alate.

¹⁵ McKinsey Global Institute (2017), Artificial Intelligence, The Next Digital Frontier?, June, pp. 4-6.

U cilju borbe protiv dubokih lažnih tehnologija, DARPA je pokrenula projekat Medijska forenzika (*MediFor*), koja nastoji „automatski detektovati manipulacije, pružiti detaljne informacije o tome kako su te manipulacije izvršene i razlog za ukupni integritet vizuelnih medija“¹⁶, razvio je neke početne alate za identifikaciju falsifikata proizvedenih od strane AI. DARPA planira da održi sljedeće aktivnosti na takmičenjima kako bi se osiguralo da forenzički alati drže korak sa dubokim lažnim tehnologijama, što je planirano za 2019. godinu.

Vještačka inteligencija se takođe može koristiti za stvaranje punih “digitalnih obrazaca života”, u kojima je digitalni “otisak” pojedinca “spojen i usklađen s istorijom kupovine, kreditnim izvještajima, profesionalnim biografijama i pretplatama” kako bi se stvorio sveobuhvatni profil ponašanja pripadnika službi, osumnjičenih obaveštajnih službenika, vladinih zvaničnika ili privatnih građana. Kao i u slučaju dubokih krivotvorina, ove informacije bi se mogle koristiti za ciljane operacije uticaja ili ucjene.¹⁷

3.1.5. Komanda i kontrola

Američka vojska npr. nastoji da iskoristi analitički potencijal AI u oblasti komandovanja i kontrole. Vazduhoplovne snage razvijaju sistem za višenamjensko komandovanje i kontrolu (MDC2), koji ima za cilj da centralizuje planiranje i izvođenje vazdušnih, svemirskih, kibernetičkih, morskih i kopnenih operacija. U bliskoj budućnosti, AI se može koristiti za spajanje podataka sa senzora u svim ovim domenima da bi se stvorio jedan izvor informacija, poznat i kao „zajednička operativna slika“, za donosiocima odluka. Trenutno, informacije koje su na raspolaganju donosiocima odluka dolaze u različitim oblicima formata sa više platformi, često sa viškom ili nerješanim neusaglašenjima.¹⁸

Zajednički omogućena operativna slika teoretski bi kombinovala ove informacije u jedan prikaz, pružajući sveobuhvatnu sliku prijateljskih i neprijateljskih snaga, i automatski rješavajući razlike od ulaznih podataka. Iako je MDC2 još uvijek u fazi razvoja koncepta, Air

¹⁶ Allen G., Chan, T. (2017), *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, July, p. 47.

¹⁷ Mills, S. (2017), Presentation at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7, str. 74.

¹⁸ Allen G., Chan, T. (2017), *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, July, p. 47.

Force radi sa Lockheed Martinom, Harrisom i nekoliko AI start-upova kako bi razvili takvu sposobnost spajanja podataka. Serija ratnih igara 2018. godine nastojala je da se usavrše zahtjevi za ovaj projekat. Slično tome, DARPA-in program *Mosaic Warfare* teži da iskoristi AI za koordinaciju autonomnih snaga i dinamičko generisanje multidomenskih komandnih i kontrolnih čvorova.

Budući da se AI sistemi mogu koristiti za identifikaciju komunikacija od strane protivnika i pronalaze alternativne načine distribucije informacija. Kako složenost AI sistema sazrijeva, AI algoritmi mogu takođe biti sposobni da obezbjede komandantima meni održivih pravaca djelovanja zasnovanih na real-time analizi borbenog prostora, koji će omogućiti bržu adaptaciju na složene događaje. Mnogi analitičari vjeruju da bi ova oblast razvoja AI mogla biti posebno posljedična, s potencijalom da se poboljša kvalitet i ubrza donošenje odluka u vrijeme rata.

3.1.6. Poluautonomna i autonomna vozila

Sve vojne službe razvijenih zemalja svijeta rade na uvođenju AI u polu-autonomna i autonomna vozila, uključujući borbene avione, kopnena vozila i brodove. AI aplikacije u ovoj oblasti su slične komercijalnim poluautonomnim vozilima, koji koriste AI tehnologije da opažaju okolinu, prepoznaju prepreke, podatke o senzorima, planiraju navigaciju i čak komuniciraju sa drugim vozilima.

Laboratorija za istraživanje vazduhoplovstva u SAD završila je dvije faze testiranja svog programa Loyal Wingman, koji spaja starije generacije borbenih avione (u ovom slučaju F-16) sa korištenim F-35 ili F-22. Tokom ovog događaja, nenaseljena testna platforma F-16 autonomno je reagovala na događaje koji nisu bili programirani, kao što su vremenske prilike i nepredviđene prepreke. Kako program napreduje, AI može omogućiti „lojalnom lovcu“ da izvrši zadatke za svoj nastanjeni let, kao što su ometanje elektronskih pretnji ili nošenje dodatnog oružja.¹⁹

¹⁹ Mills, S. (2017), Presentation at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7, str. 78.

Vojska i marinski korpus testirali su prototipove sličnih vozila koja prate vojnike ili vozila oko bojišta kako bi ostvarili nezavisne zadatke. Na primjer, višenamjenski taktički transport marinaca (MUTT) je vozilo s daljinskim upravljanjem, veličine TV-a sposoban da nosi stotine funti dodatne opreme. Iako sistem nije autonoman u svojoj trenutnoj konfiguraciji, Marinski korpus namjerava da naknadni sistemi imaju veću nezavisnost. Isto tako, vojska planira da pokrene broj robotskih borbenih vozila (RCV) sa različitim tipovima autonomne funkcionalnosti, uključujući navigaciju, nadzor i uklanjanje IED-a. Ovi sistemi će biti raspoređeni kao „krilata tehnička rješenja“ za opciono naseljeno kopneno vozilo sljedeće generacije, predviđeno za početne ocjene vojnika u FI2020.²⁰

Slika 2. DARPA primjer „AI vojnika“ po kome AI pomaže u sprečavanju povreda kod vojnika i pospješuje njihove performanse²¹



DARPA je dovršila testiranje prototipa bespilotne plovne trake Anti-Submarine Warfare Continuous Trail, ili „Sea Hunter“, početkom 2018. godine prije nego što je prešla razvoj programa u Office of Naval Research. Ako Sea Hunter uđe u službu, to bi mornarici omogućilo sposobnost autonomnog kretanja otvorenim morem, zamjene modularnih tereta i koordinacije

²⁰ Mills, S. (2017), Presentation at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7, str. 78.

²¹ <https://www.army.mil/e2/c/images/2014/05/05/343431/size0.jpg>

misija s drugim bespilotnim plovilima - sve dok osigurava kontinuirano pokrivanje podmornica mjesecima u isto vrijeme.

Neki analitičari procjenjuju da bi Sea Hunter koštao oko 20.000 dolara dnevno za rad, za razliku od oko 700.000 dolara za tradicionalno nastanjeni razarač. DOD testira druge sposobnosti koje se koriste u AI kako bi omogućile kooperativno ponašanje ili rojenje.²²

Slika 3. Primjer autonomnog vozila razvijenog od strane DARPA²³



„Rojstvo“ („Swarming“) je jedinstveni podskup autonomnog razvoja vozila, sa konceptima koji se kreću od velikih formacija jeftinih vozila dizajniranih da prevladaju odbrambene sisteme do malih eskadrila, vozila koja saraduju kako bi obezbedili elektronski napad, podršku za vatru i lokalizovane mreže za navigaciju i komunikaciju formacije trupa (kao roj insekata, po čemu je sistem i dobio ime). Trenutno se razvija nekoliko različitih rojevačkih sposobnosti. Na primjer, u novembru 2016. godine, mornarica je završila testiranje roja od pet bespilotnih brodova koji su zajednički patrolirali dijelom od 4 do 4 milje zaliva Chesapeake i presreli brod „uljez“. Rezultati ovog eksperimenta mogu dovesti do razvoja AI tehnologije prilagođene za odbranu luka, lovnih podmornica ili izviđanje pred većim brodovima. Mornarica

²² Mills, S. (2017), Presentation at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7, str. 80.

²³ <https://cdn.mainichi.jp/vol1/2016/08/26/20160826p2a00m0na020000p/9.jpg?1>

takođe planira testirati rojeve podvodnih trutova, a Kancelarija za strateške sposobnosti SAD uspješno je testirala roj od 103 mikro drona „samoubica“. ²⁴

3.2. Smrtonosni autonomni sistemi oružja

Smrtonosni autonomni sistemi oružja (*Lethal Autonomous Weapon Systems - LAWS*) su posebna klasa sistema naoružanja sposobna da samostalno identifikuje cilj i da koristi sistem naoružanja, koji se uključuje i uništava protivnika bez ljudske interakcije. Tehnologija podrazumijeva sistem kompjuterskog vida i napredne algoritme mašinskog učenja da klasifikuju objekat kao neprijateljske, donesu odluku o angažovanju i usmjere oružje do cilja. Ova mogućnost omogućava sistemu da radi u okruženjima sa komunikacijom, degradiranom ili odbijenom, gdje tradicionalni sistemi možda neće moći da rade. ²⁵

Slika 4. Primjer smrtonosnog autonomnog sistema oružja „Robot killer“²⁶



Direktiva Ministarstva odbrane SAD 3009 zahtjeva da svi sistemi bazirani na AI, bez obzira na klasifikaciju, budu dizajnirani tako da omoguće komandantima i operaterima da

²⁴ Mills, S. (2017), Presentation at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7, str. 81.

²⁵ Ilachinski, A. (2017), *AI, Robots, and Swarms, Issues, Questions, and Recommended Studies*, Center for Naval Analysis, January, p. 6.

²⁶ <https://thedefensepost.com/wp-content/uploads/2017/11/defender-autonomous-robot-081118-F-1025B-001-1170x610.jpg>

sprovedu odgovarajuće nivoe ljudskog rasuđivanja nad upotrebom sile i da uspješno završe proces pregleda oružja. Sve promjene u operativnom stanju sistema zahtjevaju da sistem ponovo prođe kroz proces pregleda oružja kako bi se osiguralo da je sistem zadržao sposobnost da funkcioniše kako je planirano.

Autonomno oružje i ograničeni tip poluautonomnog oružja moraju biti dodatno odobreni i prije razvoja i na terenu od strane pod-sekretara za odbranu; podsekretara odbrane za nabavku, tehnologiju i logistiku; i predsjedavajućeg Zajedničkog štaba. Autonomna oružja pod nadzorom ljudi koja se koriste za odbranu postrojenja ili platformi sa ljudskom posadom i autonomna oružja koja primjenjuju nesmrtonosnu, ne-kinetičku silu, kao što su neki oblici elektronskog napada, na materijalne ciljeve su takođe predmet razmatranja.²⁷

3.3. Izazovi integracije vojne vještačke inteligencije

Od doba hladnog rata do nedavno, većina glavnih tehnologija vezanih za odbranu, uključujući nuklearnu tehnologiju, sistem globalnog pozicioniranja (GPS) i internet, prvi su razvijeni od strane vladinih programa prije nego što su se kasnije šire u komercijalni sektor.

Zaista, DARPA-ina Inicijativa za strateško računarstvo uložila je više od milijardu dolara u periodu od 1983. do 1993. godine da bi razvila oblast vještačke inteligencije za vojne primjene, ali je inicijativa na kraju otkazana zbog sporijeg napretka nego što se očekivalo. Uočavajući ovu dinamiku, jedan stručnjak za AI je izjavio: Neobično je imati tehnologiju koja je tako strateški važna da se komercijalno razvija u relativno malom broju kompanija. Pored pomaka u izvorima finansiranja, niz izazova vezanih za tehnologiju i proces, ljudstvo i kultura nastavljaju da ometaju usvajanje AI u vojne svrhe.²⁸

²⁷ Ilachinski, A. (2017), *AI, Robots, and Swarms, Issues, Questions, and Recommended Studies*, Center for Naval Analysis, January, p. 6.

²⁸ Ilachinski, A. (2017), *AI, Robots, and Swarms, Issues, Questions, and Recommended Studies*, Center for Naval Analysis, January, p. 8.

3.3.1. Tehnologija

Postoji velika razlika u lakoći prilagodljivosti komercijalne AI tehnologije u vojne svrhe. Na primjer, gore pomenuti algoritmi održavanja vazduhoplova, od kojih su mnogi prvobitno razvili za komercijalni sektor, vjerovatno će zahtjevati samo mala prilagođavanja podataka da bi se uzele u obzir razlike između tipova aviona. U drugim okolnostima, potrebna su značajna prilagođavanja zbog razlika između strukturiranih civilnih sredina za koje je tehnologija prvobitno razvijena i složenijih borbenih okruženja. Na primjer, komercijalna polu-autonomna vozila su uglavnom razvijena u okruženjima bogatih podacima, sa pouzdanim GPS pozicijama, sveobuhvatnim mapiranjem terena i ažuriranim informacijama o saobraćaju i vremenskim uslovima dobijenim iz drugih umreženih vozila. Vojna varijanta takvog vozila trebala bi biti u stanju da radi na lokacijama gdje su podaci o kartama relativno siromašni i gdje GPS pozicioniranje može biti neupotrebljivo zbog ometanja protivnika. Štaviše, poluautonomna ili autonomna vojna kopnena vozila bi vjerovatno trebala mogućnost da se kreću „off-road“ na neravnom terenu - sposobnost koja nije svojstvena većini komercijalnih vozila.²⁹

3.3.2. Proces i postupci

Postojanje AI procesa - uključujući one koji se odnose na standarde sigurnosti i učinka, akvizicije i prava intelektualne svojine i podataka - predstavlja još jedan izazov za integraciju vojne AI. Često, civilni i vojni standardi sigurnosti i učinka ili nisu usklađeni ili nisu lako prenosivi. Stopa neuspjeha koja se smatra prihvatljivom za civilnu primjenu AI može biti izvan tolerancija u borbenom okruženju - ili obrnuto. Pored toga, nedavno istraživanje je zaključilo da će nepredvidivi modovi otkazivanja AI biti pogoršani u složenim okruženjima, kao što su oni koji se nalaze u borbi.

Zajedno, ovi faktori mogu stvoriti još jednu barijeru za nesmetan prenos komercijalno razvijene AI tehnologije. Tehnologija u vojsci će možda morati da prilagodi svoj proces akvizicije kako bi se odgovorilo na brzo razvijajuće tehnologije kao što je AI. Interna studija

²⁹ Ilachinski, A. (2017), *AI, Robots, and Swarms, Issues, Questions, and Recommended Studies*, Center for Naval Analysis, January, p. 11.

procesa u 2017. godini je utvrdila da je potrebno prosječno 91 mjesec da se krene od početne analize alternativa, definišući zahtjeve za sistem, na početnu operativnu sposobnost. Nasuprot tome, komercijalne kompanije obično izvršavaju iterativni proces razvoja za softverske sisteme kao što je AI, isporučujući proizvod za šest do devet mjeseci. Studija o vladinoj odgovornosti (GAO) koja je obuhvatila 12 ispitanika kompanije koje se odluče da ne posluju sa DOD-om, zaključila je da je svih 12 navelo složenost procesa nabavke odbrane kao obrazloženje za njihovu odluku.

Kao prvi korak u rješavanju ovog problema, DOD (*USA Department of Defence*) je stvorio brojne mogućnosti za „brze akvizicije“, uključujući Kancelariju za strateške sposobnosti, Odjeljenje za inovacije u odbrani i Project Maven, kako bi se ubrzao vremenski okvir za akvizicije i pojednostavili obimni procesi. Project Maven, na primjer, osnovan je u aprilu 2017; u decembru, tim je u borbenim uslovima ušao u komercijalno nabavljeni prototip AI sistema. Iako neki analitičari tvrde da je ovo obećavajući razvoj, kritičari ističu da odjeljenje mora da ponovi rezultate postignute projektom Maven u opsegu i implementaciji sveobuhvatnije reforme akvizicija.

Kompanije za komercijalnu tehnologiju su često nerado partneri sa DOD-om (*USA Department of Defence*) zbog zabrinutosti oko prava intelektualne svojine i prava na podatke. Kao zvanični intervjuisani za izvještaj GAO-a za 2017. o širim izazovima u vojnoj strategiji navode, uočeno je da je intelektualna svojina “životna krv” komercijalnih tehnoloških kompanija.³⁰

3.3.3. Osoblje

Neki izvještaji ukazuju da se DOD na primjer i odbrambena industrija takođe suočavaju sa izazovima kada je u pitanju regrutovanje i zadržavanje osoblja sa ekspertizom u AI zbog finansiranja istraživanja i plata koje značajno zaostaju za onima u komercijalnim kompanijama. Drugi izvještaji ukazuju na to da takvi izazovi proizilaze iz kvaliteta - faktora života, kao i iz uvjerenja među mnogim tehnološkim radnicima da mogu da postignu velike promjene brže i bolje izvan vlade nego unutar nje.

³⁰ Department of Defense (2017), *Joint Concept for Robotic and Autonomous Systems*, p. A-3.

Bez obzira na to, posmatrači primjećuju da ako DOD i odbrambena industrija ne mogu da regrutuju i zadržati odgovarajuće stručnjake, vojne AI aplikacije mogu biti odložene, nedostatne ili nedostaju odgovarajuće zaštitne mjere i testiranja.³¹

Za rješavanje ovih izazova, Obamina administracija je pokrenula digitalni servis za odbranu 2015. kao sredstvo zapošljavanja tehnoloških radnika iz privatnog sektora da služi u DOD-u jednu do dvije godine. Slično tome, bivši zamjenik sekretara za odbranu Bob Work predložio je “AI Training Corps”, u kojem bi DOD platio za visoko tehničko obrazovanje u zamjenu za dva dana mjesečno obuke u državnim sistemima i dvije sedmice godišnje za velike vježbe. Učesnici u programu mogli bi dodatno biti pozvani u državnu službu u slučaju vanredne situacije na nacionalnom nivou. Drugi analitičari preporučili su uspostavljanje novih vojnih obuka i specijalističkih specijalnosti za kultiviranje talenta AI, kao i stvaranje vladinih stipendija i ubrzanih promidžbenih tragova, tj. nagraditi najtalentovanije tehnološke radnike.³²

3.3.4. Kultura

Očigledna kulturna podjela između ministarstava odbrane i komercijalnih tehnoloških kompanija takođe može predstavljati izazove za usvajanje AI. Nedavno istraživanje vodstva u nekoliko vodećih kompanija u Silikonskoj dolini pokazalo je da je skoro 80% učesnika ocijenilo odnos zajednice komercijalnih tehnologija sa DOD-om kao lošim ili veoma lošim.³³ To je bilo zbog više faktora, uključujući izazove procesa, percepcije međusobnog nepovjerenja i razlike između DOD-a i struktura komercijalnih podsticaja. Štaviše, neke kompanije odbijaju da rade sa DOD-om zbog etičkih zabrinutosti zbog vladine upotrebe AI u sistemima nadzora ili oružja. Značajno je da je Google otkazao postojeće vladine ugovore za dvije robotičke kompanije koje je kupio - Boston Dynamics i Schaft - i zabranio je budući rad vlade za DeepMind, pokretanje AI softvera koje je kupio Google.

U maju 2018. Google zaposleni su uspješno lobirali da se kompanija povuče iz projekta Maven i suzdrži se od dalje saradnje sa DOD. Ostale kompanije, međutim, obećale su da će

³¹ Department of Defense (2017), *Joint Concept for Robotic and Autonomous Systems*, p. A-3.

³² Scharre, P., Horowitz, M. (2015), *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February, pp. 6-7.

³³ Scharre, P., Horowitz, M. (2015), *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February, pp. 6-7.

nastaviti da podržavaju ugovore o DOD-u, sa izvršnim direktorom Amazona Jeffom Bezosom koji je naglasio da ako velike tehnološke kompanije okrenu leđa američkom Ministarstvu odbrane, ova zemlja će biti u nevolji.

Kulturni faktori unutar samog odbrambenog objekta takođe mogu ometati integraciju AI. Integracija AI u postojeće sisteme mijenja standardizovane procedure i nadograđuje dobro definisane uloge osoblja. Članovi Projekta Maven prijavili su otpor prema integraciji vještačke inteligencije jer integracija može biti ometajuća, a da pritom ne pruža uvijek prepoznatljivu korist.

Zamjenik direktora za razvoj tehnologije CIA-e Dawn Meierriecks je također izrazio zabrinutost zbog spremnosti viših rukovodilaca da prihvate analizu generisanu od AI tvrdeći da kultura odbijanja odbrambenog sistema može predstavljati veći izazov za buduću konkurentnost nego tempo razvoja protivničke tehnologije. Konačno, neki analitičari su zabrinuti da DOD neće iskoristiti potencijal AI za proizvodnju sistema za savremeno ratovanje, koristi koje će mijenjati igru i umjesto toga će jednostavno koristiti AI za postepeno poboljšanje postojećih procesa ili jačanje postojećih operativnih koncepata. Štaviše, službe mogu odbaciti određene AI aplikacije ako tehnologija ugrožava hardver ili misije koje favorizuju uslugu. Članovi Kongresa mogu istražiti složenu interakciju ovih faktora, pošto DOD prelazi početne faze usvajanja AI.³⁴

3.4. Mogućnosti i izazovi vještačke inteligencije u vojsci

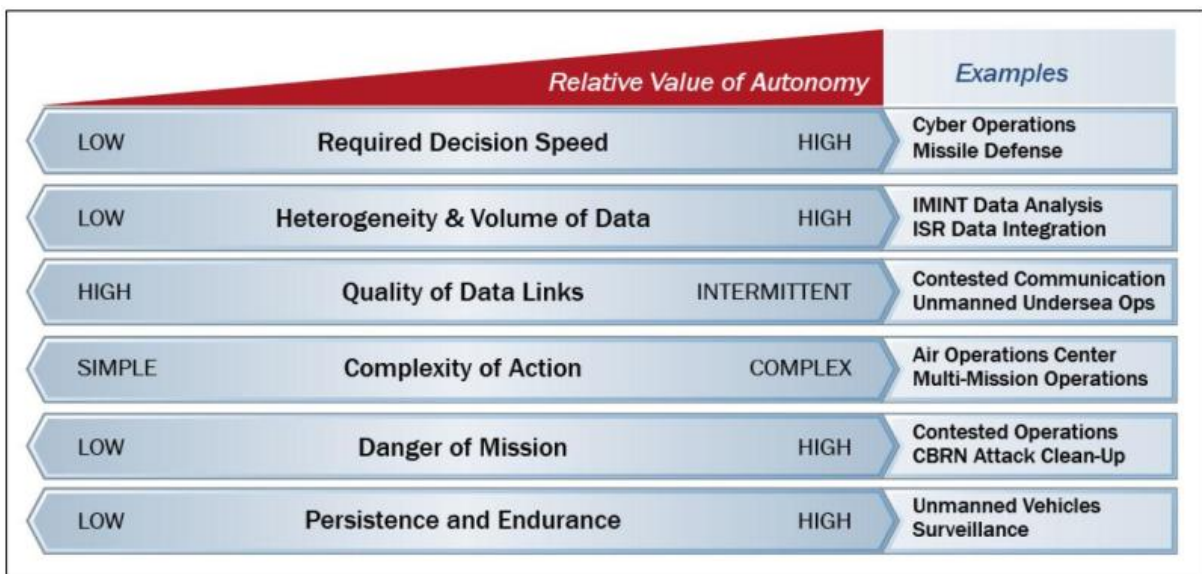
AI predstavlja niz jedinstvenih mogućnosti i izazova u kontekstu nacionalne sigurnosti. Međutim, njegov konačni uticaj će vjerovatno biti određen stepenom do kojeg su programeri, uz pomoć kreatora politike, u mogućnosti da maksimiziraju svoje snage, dok identifikuju opcije za ograničavanje svojih ranjivosti.

³⁴ Scharre, P., Horowitz, M. (2015), *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February, pp. 6-7.

3.4.1. Autonomija

Mnogi autonomni sistemi uključuju AI u nekom obliku. Takvi sistemi bili su centralni fokus “Treće ofset strategije” administracije Obame, okvir za očuvanje tehnološke prednosti američke vojske protiv globalnih konkurenata. U zavisnosti od zadatka, autonomni sistemi su sposobni da uvećaju ili zamijene ljude, oslobađajući ih za više složen i kognitivno zahtjevan rad. Generalno, stručnjaci tvrde da vojska ima značajne koristi od autonomnih sistema zamjenjujući ljude zadacima koji su „tupi, opasni ili prljavi“.³⁵ Specifični primjeri autonomije u vojnim sistemima uključuju sisteme koji provode dugotrajne obavještajne podatke i analiza, čišćenje okruženja zagađenih hemijskim oružjem ili rute za improvizovane eksplozivne naprave. U tim ulogama, autonomni sistemi mogu smanjiti rizik za ratnike i smanjiti troškove, pružajući raspon vrijednosti misijama DOD, kao što je prikazano na slici 1. Neki analitičari tvrde da ove prednosti stvaraju “taktičku i stratešku neophodnost”, kao i “moralnu obavezu” za razvoj autonomnih sistema.³⁶

Slika 5. Vrijednost autonomije za misije DOD (USA Department of Defence)³⁷



³⁵ Scharre, P., Horowitz, M. (2015), *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February 2015, pp. 6-7.

³⁶ U.S. Congress (2018), House of Representatives Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies*, 115th Cong., 2nd sess., January 9, str. 40.

³⁷ <https://www.acq.osd.mil/dsb/reports/2010s/DSBSS15.pdf>

3.4.2. Brzina i izdržljivost

AI uvodi jedinstven način rada u borbi u ekstremima vremenske skale. Ona obezbeđuje sisteme sa sposobnošću da reaguju na brzinu gigaherca, što zauzvrat ima potencijal da dramatično ubrza sveukupni tempo borbe. Kao što je objašnjeno u daljem tekstu, neki analitičari tvrde da bi drastično povećanje ritma borbe moglo da destabilizuje - posebno ako ona prevazilazi ljudsku sposobnost da razumije i kontroliše događaje - i može da poveća destruktivni potencijal sistema u slučaju gubitka kontrole sistema. Uprkos ovom riziku, neki tvrde da će brzina donijeti konačnu prednost ratovanja, što će opet stvoriti pritiske za široko usvajanje vojnih AI aplikacija. Pored toga, AI sistemi mogu pružiti pogodnosti u dugotrajnim zadacima koji prevazilaze ljudsku izdržljivost. Na primjer, AI sistemi mogu omogućiti prikupljanje obavještajnih podataka na velikim područjima u dužim vremenskim periodima, kao i sposobnost autonomnog otkrivanja anomalija i kategorizacije ponašanja.³⁸

3.4.3. Skaliranje

AI ima potencijal da obezbjedi efekat multipliciranja sile tako što će povećati ljudske sposobnosti i ubaciti manje skupe vojne sisteme sa povećanim sposobnostima. Na primjer, iako pojedinačni jeftini bespilotni avion može biti nemoćan u odnosu na visokotehnološki sistem kao što je F-35 borbeni avion, eskadrila takvih bespilotnih letilica mogla bi potencijalno preplaviti visokotehnološke sisteme, generišući značajne uštede troškova i potencijalno pretvarajući neke trenutne platforme koje su zastarile. Sistemi AI takođe mogu povećati produktivnost pojedinih serviseru jer sistemi preuzimaju rutinske zadatke ili omogućavaju taktike kao što su rojenje koje zahtjevaju minimalno ljudsko učešće. Na kraju, neki analitičari upozoravaju da bi širenje sistema AI moglo odvojiti vojnu moć od stanovništva, veličinu i ekonomsku snagu. Ovo razdvajanje može omogućiti manjim zemljama i nedržavnim akterima

³⁸ U.S. Congress (2018), House of Representatives Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies*, 115th Cong., 2nd sess., January 9, str. 40.

da imaju neproporcionalno veliki uticaj na bojno polje ako mogu da iskoriste efekte skaliranja AI.³⁹

3.4.4. Superiornost informacija

AI može ponuditi sredstvo za suočavanje sa eksponencijalnim povećanjem količine podataka dostupnih za analizu. Prema jednom izvoru DOD-a, vojska upravlja preko 11.000 bespilotnih letjelica, od kojih svaka zabilježi svaki dan "više od tri sezone NFL-a" snimaka visoke definicije.⁴⁰ Međutim, odjel nema dovoljno ljudi ili adekvatan sistem za pročešljavanje podataka kako bi se dobila analiza obavještajnih podataka. Ovo pitanje će vjerovatno biti pogoršano u budućnosti, kako se podaci nastavljaju akumulirati. Prema jednoj studiji, do 2020. godine svako ljudsko biće na planeti će generisati 1.7 megabajta informacija svake sekunde, rastući globalni skup podataka sa 4.4 zetabajta danas na skoro 44.0 zetabajta.

Sposobni inteligentni sistemi mogu pružiti mogućnost integracije i sortiranja kroz velike podatke iz različitih izvora i geografskih lokacija za identifikaciju obrazaca i isticanje korisnih informacija, značajno poboljšanje analize inteligencije. Osim toga, algoritmi za inteligenciju mogu generisati svoje vlastite podatke za daljnju analizu, izvršavajući zadatke kao što su konverzija nestrukturiranih informacija iz anketa, finansijskih podataka, i izborne rezultate u pisane izvještaje. Na taj način, AI alati ovog tipa imaju potencijal da pruže prednost ratnim dejstvima poboljšanjem kvaliteta informacija dostupnih donosiocima odluka.⁴¹

³⁹ U.S. Congress (2018), House of Representatives Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies*, 115th Cong., 2nd sess., January 9, str. 40.

⁴⁰ Clark, C. (2017), "Our Artificial Intelligence 'Sputnik Moment' is Now: Eric Schmidt and Bob Work," *Breaking Defense*, November 1.

– <https://breakingdefense.com/2017/11/our-artificial-intelligence-sputnik-moment-is-now-eric-schmidt-bob-work/>

⁴¹ Clark, C. (2017), "Our Artificial Intelligence 'Sputnik Moment' is Now: Eric Schmidt and Bob Work," *Breaking Defense*, November 1.

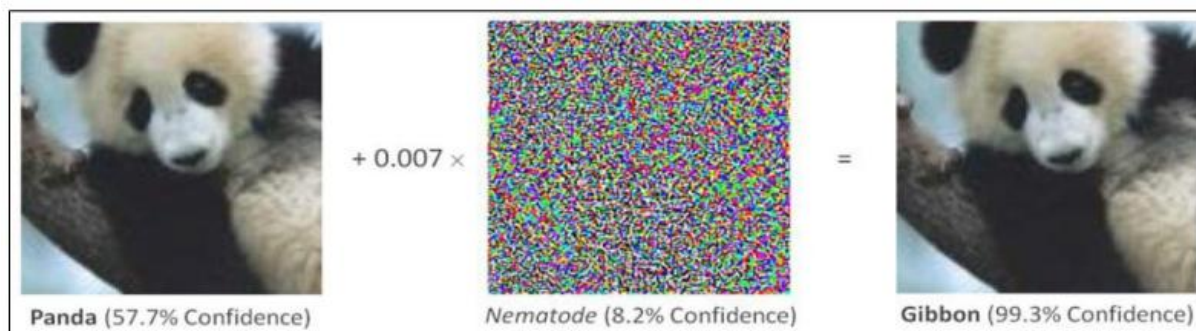
3.4.5. Predvidljivost

AI algoritmi često proizvode nepredvidive i nekonvencionalne rezultate. U martu 2016. godine, AI kompanija DeepMind je kreirala algoritam za igranje igara AlphaGo, koji je pobijedio svjetskog prvaka Go player, Lee Sedola, četiri utakmice naprema jednu. Nakon meča, Sedol je komentarisao da AlphaGo pravi iznenađujuće i inovativne poteze, a drugi stručnjaci Go-a naknadno su izjavili da je AlphaGo preokrenuo nagomilanu mudrost u igri. AI sposobnost da proizvede slične nekonvencionalne rezultate u vojnom kontekstu može pružiti prednost u borbi, posebno ako ti rezultati iznenade protivnika.

Međutim, AI sistemi mogu da propadnu na neočekivane načine, s tim da neki analitičari svoje ponašanje opisuju kao “krhki i nefleksibilni”. Dr. Arati Prabhakar, bivši direktor DARPA-e, komentarisao je to na način: “Kada pogledamo šta se dešava sa AI, vidimo nešto što je veoma moćno, ali takođe vidimo tehnologiju koja je još uvek prilično ograničena, problem je u tome što kada je pogrešno, to je pogrešno na način da nijedan čovjek tako nešto nikada ne bi pogriješio.”⁴²

⁴² Clark, C. (2017), “Our Artificial Intelligence ‘Sputnik Moment’ is Now: Eric Schmidt and Bob Work,” *Breaking Defense*, November 1.

Slika 6. AI i greške klasifikacije slike⁴³



Algoritmi za prepoznavanje slika zasnovani na AI nadmašili su ljudske performanse u 2010. najskorije postizanje stope greške od 2,5% u odnosu na prosječnu stopu ljudske greške od 5%; međutim, neki često citirani eksperimenti sa ovim sistemima pokazuju svoj kapacitet za neuspjeh. Kao što je prikazano na slici 6, istraživači su kombinovali sliku koju je AI sistem ispravno identifikovao kao pandu sa slučajnim izobličenjem koje je računar označio kao „nematode”. kombinovana slika je nevidljiva ljudskim očima, ali AI sistem je označio sliku kao „gibbon# sa 99.3% tačnosti.

U drugom eksperimentu, sistem AI opisao je sliku na slici 7 kao “dječak drži bejzbol palicu”, pokazujući nemogućnost algoritma da razumije kontekst. Neki stručnjaci upozoravaju da AI može da radi sa različitim pretpostavkama o životnoj sredini, nego što to rade ljudi, Slično tome, AI sistemi mogu biti predmet algoritamske pristranosti kao rezultat njihovih podataka o obuci. Na primjer, istraživači su više puta otkrili slučajeve rasne pristranosti u programima za prepoznavanje lica AI zbog nedostatka raznolikosti u slikama na kojima su sistemi obučavani, dok su neki programi obrade prirodnog jezika razvili rodnu pristranost. To bi moglo da ima značajne implikacije za AI aplikacije u vojnom kontekstu, posebno ako takve predrasude ostanu neotkrivene i uključene u sisteme sa smrtonosnim efektima.⁴⁴

⁴³ <https://www.darpa.mil/attachments/AIFull.pdf>

⁴⁴ Clark, C. (2017), “Our Artificial Intelligence ‘Sputnik Moment’ is Now: Eric Schmidt and Bob Work,” *Breaking Defense*, November 1.

Slika 7. AI i kontekst „Dječak drži bejzbol palicu“⁴⁵



“Prilagodljivost domena”, ili sposobnost AI sistema da se prilagodi između dva različita okruženja, također može predstavljati izazove za vojsku. Na primjer, jedan sistem AI razvijen da prepozna i razumije online tekst, obučan prvenstveno na dokumentima na formalnom jeziku kao što su Wikipedia članci. Sistem je kasnije bio u nemogućnosti da tumači više neformalnog jezika u postovima na Twitteru. Neuspjeh adaptabilnosti domena može se desiti kada se sistemi razvijeni u civilnom okruženju prenesu u borbeno okruženje.

Kvarovi sistema AI mogu da stvore značajan rizik ako se sistemi primjenjuju na skali. Jedan analitičar je primijetio da, iako ljudi nisu imuni na greške, njihove greške se obično prave na individualnoj osnovi i one su uvek različite. Međutim, AI sistemi imaju potencijal da propadnu istovremeno i na isti način, potencijalno proizvodeći velike ili destruktivne efekte. Ostali neočekivani rezultati mogu nastati kada US AI sistemi interaguju sa protivnikovim AI sistemima obučanim na različitim skupovima podataka sa različitim projektnim parametrima i kulturne predrasude.

Analitičari upozoravaju da, ako vojska požuruje da primjeni tehnologiju pre nego što stekne sveobuhvatno razumijevanje potencijalnih opasnosti, može doći do „tehničkog duga“, termina koji se odnosi na efekat uvođenja sistema AI koji imaju minimalni rizik pojedinačno, ali koji uslovljavaju kolektivni rizik na interakcije između sistema. Ovaj rizik mogao bi se dodatno pogoršati u slučaju utrke u oružju sa AI.⁴⁶

⁴⁵ <https://www.darpa.mil/attachments/AIFull.pdf>

⁴⁶ Corrigan, J. (2018), “U.S. Needs a National Strategy for Artificial Intelligence, Lawmakers and Experts Say,” *Defense One*, July 14.

Dalje komplikujući pitanja predvidljivosti, tipovi AI algoritama koji imaju najveće performanse trenutno nisu u stanju da objasne svoje procese. Na primjer, Google je stvorio sistem za identifikaciju mačaka, koji je postigao impresivne rezultate u identifikaciji mačaka na YouTube-u; međutim, nijedan od programera sistema nije bio u stanju da odredi koje osobine mačke sistem koristi u svom procesu identifikacije. Ovaj nedostatak takozvane “objašnjivosti” je uobičajen za sve takve algoritme AI. Da bi se riješio ovaj problem, DARPA provodi petogodišnji istraživački napor da proizvede objašnjive alate AI.

Druge istraživačke organizacije takođe pokušavaju da urade analizu ovih tipova algoritama unazad kako bi bolje razumjeli svoje unutrašnje procese. U jednoj takvoj studiji, istraživači su analizirali program koji je dizajniran da identifikuje zavjese i otkrio da je AI algoritam prvo tražio krevet, a ne prozor, u kom trenutku je prestao da traži sliku. Istraživači su kasnije saznali da je to zbog toga što je većina slika u setu podataka o obuci koje su sadržavale zavjese spavaće sobe. Projekat je pokazao mogućnost da setovi obuke nenamjerno unesu greške u sistem koji korisnici ne mogu odmah prepoznati ili razumjeti.

Objašnjenje može stvoriti dodatna pitanja u vojnom kontekstu, jer neprozirnost rasuđivanja inteligencije može dovesti do toga da operatori imaju previše ili premalo povjerenja u sistem. Neki analitičari su posebno zabrinuti da bi ljudi mogli biti nespremni da donesu odluku zasnovanu isključivo na AI analizi ako ne razumiju kako je mašina proizvela rješenje. Dawn Meierriecks, zamjenik direktora za nauku i tehnologiju u CIA-i, izrazila je zabrinutost, tvrdeći, “dok mi AI ne pokaže svoj domaći zadatak, to nije proizvod koji donosi odluku o kvalitetu odluke”. u AI sistemima.⁴⁷

Kao što studija američke vojske o ovom pitanju zaključuje, samo “razborito povjerenje” će dati konkurentsku prednost vojnim organizacijama. Dodatna pitanja interakcije između čovjeka i mašine koja mogu biti izazvana nedovoljnom objašnjenošću u vojnom kontekstu uključuju sljedeće:⁴⁸

– <https://www.defenseone.com/technology/2018/07/us-needs-national-strategy-artificial-intelligencelawmakers-and-experts-say/149644/>

⁴⁷ Corrigan, J. (2018), “U.S. Needs a National Strategy for Artificial Intelligence, Lawmakers and Experts Say,” *Defense One*, July 14.

⁴⁸ Sydney J. Freedberg, Jr. (2018), “Pentagon Rolls Out Major Cyber, AI Strategies This Summer,” *Breaking Defense*, July 17.

– <https://breakingdefense.com/2018/07/pentagon-rolls-out-major-cyber-ai-strategies-this-summer/>

- Usaglašavanje ciljeva - Ljudi i mašina moraju imati zajedničko razumijevanje cilja. Kako se vojni sistemi susreću sa dinamičnom okolinom, ciljevi će se promijeniti, a ljudsko i mašinsko se moraju prilagoditi istovremeno na osnovu zajedničke slike trenutne okoline.
- Usklađivanje zadataka - Ljudi i mašine moraju razumjeti granice prostora za donošenje odluka jednih drugih, posebno kada se ciljevi menjaju. U ovom procesu, ljudi moraju biti potpuno svjesni ograničenja dizajna stroja kako bi se zaštitili od neprikladnog povjerenja u sistem.
- Interfejs ljudske mašine - Zbog zahtjeva za pravovremene odluke u mnogim vojnim AI aplikacijama, tradicionalni mašinski interfejsi mogu usporiti performanse, ali mora postojati način da se čovjek i mašina koordiniraju u realnom vremenu kako bi izgradili povjerenje.

Konačno, mogućnost objašnjavanja mogla bi da izazove sposobnost vojske da “verifikuje i potvrdi” performanse sistema AI prije nego što se izvede teren. Zbog njihovog trenutnog nedostatka objašnjivog izlaza, AI sistemi nemaju trag revizije za vojnu testnu zajednicu da potvrdi da sistem ispunjava standarde performansi. DOD trenutno razvija okvir za testiranje životnog ciklusa AI sistema i metode izgradnje za testiranje AI sistemi u različitim okruženjima sa složenim interakcijama između ljudi i mašina.

3.4.6. Eksploatacija

Sistemi AI predstavljaju jedinstvene puteve za eksploataciju protivnika. Prvo, proliferacija AI sistema će povećati broj stvari koje se mogu hakovati, uključujući sisteme koji nose kinetičku energiju (npr. pokretna vozila), što može zauzvrat omogućiti eksplozivne akcije da izazovu smrtonosne efekte. Ovi efekti mogu biti posebno štetni ako cijela klasa AI sistema ima istu ranjivost koja se može iskoristiti. Osim toga, AI sistemi su posebno osjetljivi na krađu zbog činjenice da su gotovo u potpunosti zasnovani na softveru. Kao što jedan analitičar ističe, Kinezi će možda moći da ukradu planove za F 35, ali će im trebati godine da pronađu materijale i razviju proizvodne procese za izgradnju jednog. Nasuprot tome, ukradeni softverski kod se može odmah koristiti i reprodukovati po želji.⁴⁹

⁴⁹ Sydney J. Freedberg, Jr. (2018), “Pentagon Rolls Out Major Cyber, AI Strategies This Summer,” *Breaking Defense*, July 17.

Ovaj rizik je pojačan prirodom tehnologije dvostruke namjene i činjenicom da je istraživačka zajednica AI bila relativno otvorena za saradnju do ove tačke. Zaista, brojni AI alati razvijeni za civilnu upotrebu - ali koji bi se mogli prilagoditi za upotrebu u oružanim sistemima - bili su široko podijeljeni na neklasificiranim internet stranicama, što ih je učinilo dostupnim glavnim vojnim snagama i ne-državnim akterima.

U jednom takvom slučaju, istraživači koji su imali pristup skupu podataka o obuci i algoritmu za klasifikator slike na poluautonomnom vozilu koristili su nekoliko komada strateški postavljene trake da bi sistem identifikovao znak zaustavljanja kao znak za ograničenje brzine. U kasnijim istraživanjima, tim na MIT-u uspješno je prevario klasifikatora slike da misli da je slika mitraljez helikoptera - bez pristupa podacima ili algoritmu obuke sistema. Ove ranjivosti naglašavaju potrebu za robusnom sigurnošću podataka, sajber bezbjednošću i procesima testiranja i evaluacije.⁵⁰

3.5. Autonomna oružja i vojska

Autonomna oružja, kolokvijalno rečeno, korišćena su od Drugog svjetskog rata (npr. Pasivni akustični tragač za torpedom njemačkog Wren-a efektivno ga je učinio prvom autonomnom municijom na svijetu). Korišćena prije više od 20 godina (RK-1 Predator je korišćen kao obavještajna, nadzorna i izviđačka platforma u bivšoj Jugoslaviji), ali svoje stvarne prve primjere predstavlja tek nakon 11. septembra 2001. godine, kada su teroristički napadi bili u porastu i sve veće oslanjanje na bespilotna vozila su počela ozbiljno da dolaze u prvi plan interesovanja. Za samo 10 godina, inventar bespilotnih letelica DOD-a porastao je sa 163, u 2003. na skoro 11.000, u 2013. (i, u 2013. godini, činio je 40% svih aviona). I Sjedinjene Države su daleko od toga da budu samo zainteresovane za bespilotne letelice: po jednom

⁵⁰ Sydney J. Freedberg, Jr. (2018), "Pentagon Rolls Out Major Cyber, AI Strategies This Summer," *Breaking Defense*, July 17.

skorašnjem istraživanju najmanje 30 zemalja ima velike vojne bespilotne letilice, a naoružani dron klub je nedavno porastao na 11 zemalja u svijetu, uključujući tu i Sjedinjene Države.⁵¹

DOD je nabavio većinu svojih srednjih i većih bespilotnih letelica, MK-1/8 / 9s i RK-4s, za kampanje protiv pobunjenika u Iraku i Avganistanu, gdje je vazdušni prostor bio u velikoj mjeri nesiguran. Sada se Sjedinjene Države povlače iz tih kampanja i vojska prebacuje svoj strateški fokus na manje permisivna radna okruženja (tj. na azijsko-pacifički region) i na protivnike sa modernim sistemima protivvazdušne odbrane. Stoga se sve više naglašava razvoj novih, autonomnijih sistema koji su bolje opremljeni za opstanak u spornijim zračnim prostorima. U suštini, autonomni sistem je sistem koji može samostalno komponovati i birati između alternativnih pravaca djelovanja kako bi ostvario ciljeve na osnovu svog znanja i razumijevanja svijeta, samog sebe i lokalnog, dinamičkog konteksta. Za razliku od automatizovanih sistema, autonomni sistemi moraju biti u stanju da odgovore na situacije koje nisu unapred programirane ili predviđene prije njihovog uvođenja. Ukratko, autonomni sistemi su inherentno, i nesvodivo, vještački inteligentni roboti.⁵²

Za početak, ako i kada autonomni sistemi, u opisanom smislu, konačno stignu, oni će ponuditi razne očite prednosti ratniku. Na primjer, oni će eliminisati rizik od povrede i / ili smrti ljudskog operatera; nude slobodu od ljudskih ograničenja u opterećenju, umoru i stresu; i biti u stanju da asimiliraju visoke podatke o volumenu i donesu „odluke“ na osnovu vremenskih skala koje daleko prevazilaze ljudske sposobnosti. Ako se u mješavinu dodaju robotski rojevi, potpuno se otvaraju potpuno novi prostori za misije, npr. široko područje, dugotrajnost, nadzor; umreženo, adaptivno elektronsko ometanje; i koordinisani napad.

Postoje i brojne prednosti korišćenja rojeva, a ne pojedinačnih robota, uključujući: efikasnost (ako se zadaci mogu dekomponovati i izvoditi paralelno), raspodjeljena akcija (više istovremenih kooperativnih akcija može se vršiti na različitim mjestima u isto vrijeme) i tolerancija kvarova (neuspjeh jednog robota unutar grupe ne znači nužno da određeni zadatak ne može biti ostvaren).

⁵¹ Velez-Green, A., Scharre, P. (2017), “The United States Can Be a World Leader in AI. Here’s How.,” *The National Interest*, November 2.

⁵² Velez-Green, A., Scharre, P. (2017), “The United States Can Be a World Leader in AI. Here’s How.,” *The National Interest*, November 2.

3.5.1. Tehnički izazovi

Dizajn i razvoj autonomnih sistema podrazumijeva značajne konceptualne i tehničke izazove, uključujući mnoge detalje, koji su često prepreka za istraživanje. Razvojni sistemi autonomnih sistema moraju se suočiti sa mnogim osnovnim problemima sa kojima se bore akademske i komercijalne AI i robotske istraživačke zajednice decenijama. Da bi preživjeli i uspješno obavljali misije, autonomni sistemi moraju biti u stanju da osjete, opažaju, otkriju, identifikuju, klasifikuju, planiraju, odlučuju i reaguju na različite prijetnje u složenim i neizvjesnim okruženjima. Dok su aspekti svih ovih “problema” riješeni u različitim stepenima, još uvijek ne postoji sistem koji bi u potpunosti obuhvatio sve te karakteristike.⁵³

Kompleksna i neizvjesna okruženja - Autonomni sistemi moraju biti u stanju da funkcionišu u kompleksnim, eventualno, a priori nepoznatim okruženjima koja posjeduju veliki broj potencijalnih stanja koja ne mogu biti unaprijed određena ili iscrpno ispitana ili testirana. Sistemi moraju biti u stanju da asimiliraju, odgovore i prilagode se dinamičkim uslovima koji nisu razmatrani tokom njihovog dizajna. Ovaj problem „skaliranja“, tj. sposobnost da se dizajniraju sistemi koji su razvijeni i testirani u statičkim i strukturiranim okruženjima, a zatim da se oni izvode kako je potrebno u dinamičkim i nestrukturiranim okruženjima je veoma kompleksan.

Emergentno ponašanje - Da bi se autonomni sistem mogao prilagoditi promjenjivim uslovima okoline, mora imati ugrađenu sposobnost učenja i to bez ljudskog nadzora. Može biti teško predvidjeti i biti u stanju objasniti a priori neočekivano, pojavljujuće ponašanje (virtualna sigurnost u dovoljno “kompleksnim” sistemima dinamičkih sistema sistema).

Interakcije čovjek-mašina / I - Operativna efikasnost autonomnih sistema će zavistiti od dinamičke interakcije između ljudskog operatera i mašine (a) u datoj okolini, i od toga kako sistem u realnom vremenu reaguje na promjene operativnih ciljeva, u saglasnosti sa sopstvenim prilagođavanjem čovjeka dinamičnim kontekstima. Urođena nepredvidljivost ljudske komponente u kolaborativnim performansama čovek-mašina samo pogoršava druge izazove koji su identifikovani na ovoj listi.

⁵³ Sydney J. Freedberg, Jr. (2018), “Pentagon Rolls Out Major Cyber, AI Strategies This Summer,” *Breaking Defense*, July 17.

Interakcije čovjek-mašina / II - Interfejs između ljudskih operatora i autonomnih sistema vjerovatno će uključivati raznolik prostor alata koji uključuju vizuelne, slušne i taktilne komponente. U svim slučajevima, postoji izazov prevođenja ljudskih ciljeva u kompjuterske instrukcije (npr. rješavanje dugogodišnjeg AI problema obrade prirodnog jezika), kao i prikazivanje "prostora za odlučivanje" u obliku koji je razumljiv ljudskom operateru (npr. dozvoljavajući operateru da odgovori na pitanje „Zašto je sistem izabrao da preduzme akciju X?“).

Kontrola - Kako se autonomni sistemi povećavaju složenosti, možemo očekivati srazmjerno smanjenje naše sposobnosti da predvidimo i kontrolišemo takve sisteme, tj. "Spektar samozadovoljstva u kompleksnosti". Kao što pokazuje opšta priroda nedavnih otkrića AI, je fundamentalni kompromis: bilo da AI može da dostigne određeni nivo performansi (npr. može da igra igru Go, ili bolje od, čovjeka), ili ljudi mogu da razumiju kako se postiže njegov učinak).⁵⁴

Pored ovih urođenih tehničkih izazova za razvoj autonomnih sistema, postoji niz pratećih izazova za sticanje, čije je porijeklo nedavna promjena u praksama nabavke vezanih za inovacije u DOD-u. Iako je vlada SAD-a oduvijek imala važnu ulogu u podsticanju istraživanja AI (npr. ARPA, DARPA, NSF, ONR), većina ključnih inovacija u AI, robotici i autonomiji sada se pokreće od strane komercijalnog sektora i brzinom da je relativno jeftin proces kupovine DOD-a oskudan za smještaj: potrebno je 91 mjesec (7,6 godina), u prosjeku, od početka analize alternativa (AoA) do početne operativne sposobnosti (IOC), kao što smo to i ranije naveli.⁵⁵ Čak i informacije o tehnološkim programima u čijim rubrikama većina AI-a stiže prirodne padove u prosjeku su 81 mjesec. Poređenja radi, imajmo na umu da je u okviru istog vremenskog perioda, komercijalna istraživačka zajednica AI prešla sa eksperimentisanja sa (prototipovima posvećenih hardverski podržanih) tehnika dubokog učenja, da bi pobijedila svjetskog šampiona u Go-u (zajedno sa postizanjem cilja) mnogo drugih velikih otkrića.

Naravno, izazovi za nabavku DOD-a, posebno za sisteme oružja koji uključuju tešku vezu između hardvera i softvera, poznati su već decenijama. Međutim, uprkos brojnim pokušajima različitih zainteresovanih strana da se pozabave ovim izazovima, proces generičke

⁵⁴ Sydney J. Freedberg, Jr. (2018), "Pentagon Rolls Out Major Cyber, AI Strategies This Summer," *Breaking Defense*, July 17.

⁵⁵ Sydney J. Freedberg, Jr. (2018), "Pentagon Rolls Out Major Cyber, AI Strategies This Summer," *Breaking Defense*, July 17.

nabavke (barem na tradicionalni institucionalni nivo) ostaje efektivno nepromijenjen. Kakav god da je napredak postignut u posljednjih nekoliko godina, više proizilazi iz zaobilaznih rješenja koje je uspostavio DOD kako bi se olakšalo „brzo sticanje“ sistema, nego od veleprodajnih promjena koje se primjenjuju na procese nabave koji se odvijaju u samom procesu nabave. Postignut je nedavni napredak, npr., Nacionalni akti o autorizaciji odbrane (NDAA / Sec 804) za 2009./2011. Godinu, nalažu novi proces nabavke IT-a, koji je, sa svoje strane, doveo do više studija Radne grupe za naučne odbrane (DSB) procesa nabavke. Ipak, značajno odsustvo u bilo kojoj od ovih DSB / TF studija je bilo kakvo izričito spominjanje autonomije.

Dalje, komplikovanje ovog pitanja je osnovna dihotomija između postojeće direktive o autonomiji Ministarstva odbrane (DOD Directive 3000.09, objavljena u novembru 2012. godine) i trenutne prakse u testiranju i evaluaciji (T&E) i verifikaciji i validaciji (V&V). Direktiva 3000.09 dalje zahtjeva da T & E / V & V procjenjuje performanse sistema, sposobnost, pouzdanost, efektivnost i pogodnost u realnim uslovima, uključujući moguće protivničke radnje, u skladu sa potencijalnim posledicama nenamernog angažovanja ili gubitka kontrole sistema. Postojeća praksa T & E / V & V ne pravi nikakav smještaj za bilo koji dio ovih navodnih zahtjeva. Među mnogim razlozima zašto su autonomni sistemi posebno teški za testiranje i validaciju su:

- složenost stanja-prostora (nemoguće je izvršiti iscrpnu pretragu ogromnog prostora mogućih „stanja“ sistema za autonomne sisteme);
- složenost fizičkog okruženja (ponašanje autonomnog sistema ne može se specifikovati mnogo manje testirano i sertifikovano in situ, već mora biti testirano u skladu sa interakcijom sa dinamičnom okolinom, prikazujući prostor sistemskih ulaza / izlaza i varijabli okruženja). kombinovano tvrdoglav);
- nepredvidljivost (u meri u kojoj su autonomni sistemi inherentno kompleksni adaptivni sistemi, može se očekivati da će se novo ili neočekivano ponašanje pojaviti prirodno i nepredvidivo u određenim dinamičkim situacijama; postojeće prakse T & E / V & V nemaju potrebnu vjernost da se nose sa problemima u nastajanju); i
- povjerenje operatera u stroj (postojeća T & E / V & V praksa je ograničena na sisteme testiranja u zatvorenim, skriptiranim okruženjima, budući da “povjerenje” nije urođena karakteristika sistema).

Povjerenje takođe podrazumijeva suočavanje sa pitanjem iskustva i / ili učenja: da bi bili efikasniji, autonomni sistemi mogu biti obdareni sposobnošću da prikupljaju informacije i uče iz iskustva. Međutim, takva sposobnost se ne može monolitno potvrditi tokom jednog vremenskog perioda „provjeri kutiju“. Umesto toga, to zahteva periodično ponovno testiranje i resertifikaciju, čija periodičnost je nužno funkcija istorije sistema i iskustva misije. Postojeće prakse T & E / V & V su potpuno neadekvatne za rješavanje ovih pitanja.

3.5.2. Definisane autonomnog segmenta vještačke inteligencije

„Autonomija“ se odnosi na mnogo veći opseg procesa od onih koji se odnose na bespilotna vozila kao fizička lica, uključujući i bezbroj faktora potrebnih za opisivanje interakcija čovjek-mašina. Predstavlja niz mogućnosti zavisnih od konteksta, koje se mogu pojaviti u različitim skalama i u različitim stepenima sofisticiranosti, koje kolektivno omogućavaju da spregnuti sistem čovjek-mašina obavlja određene zadatke. Autonomija sama po sebi ne redukuje „postojeće“ probleme; radije, redefinira, proširuje i potencijalno otvara potpuno nove prostore misija. Njegova vrijednost se može procijeniti samo u kontekstu specifičnih zahtjeva misije, radne okoline i njenog povezivanja s ljudskim operaterima.⁵⁶

Glavna prepreka razvoju autonomnih sistema naoružanja je trenutni nedostatak zajedničkog jezika pomoću kojeg AI, roboti i drugi tehnološki stručnjaci, programeri i programski menadžeri mogu komunicirati (na način koji je konzistentan sa multidimenzionalnim, kontekstualnim kontekstom, zavisne prirode). Postoji ne čak ni jednu definiciju riječi autonomija, a još manje univerzalno dogovorenu taksonomiju koja bi se mogla koristiti kao osnova za formiranje zajedničkog jezika.⁵⁷

Neke taksonomije naglašavaju detalje vezane za izlazne funkcije sistema (tj. za njegovu sposobnost odlučivanja), dok se drugi fokusiraju na izradu detaljnih razlika između ulazne funkcije, kao što je način na koji sistem prikuplja informacije i kako formuliše opcije. I dok su klizne skale korišćene za ocenjivanje između nivoa „ljudske kontrole“ koje određeni sistem

⁵⁶ Velez-Green, A., Scharre, P. (2017), “The United States Can Be a World Leader in AI. Here’s How.,” *The National Interest*, November 2.

⁵⁷ Velez-Green, A., Scharre, P. (2017), “The United States Can Be a World Leader in AI. Here’s How.,” *The National Interest*, November 2.

može da zahteva (npr. „autonomija“ sistema može biti rangirana od, recimo, 0, što znači da je pod potpunom kontrolom, do 10, što znači da je potpuno autonoman, iako, obično, bez termina koji je u potpunosti dobro definisan, praktična upotrebljivost ovih vrsta taksonomija je ograničena jer ignorišu kritički važne kontekstualne faktore.⁵⁸

3.5.3. Etička pitanja vještačke inteligencije u vojsci

Pojava autonomnog naoružanja i spektar (ako ne i realnost) smrtonosnih autonomnih sistema naoružanja (LAWS), koji mogu sami da biraju i zahvataju ciljeve, postavlja mnoštvo etičkih i moralnih pitanja. Na primjer: „Hoće li vojnici biti spremni da idu u borbu zajedno sa robotima?“ „Hoće li roboti moći da razlikuju vojne i civilne ciljeve i da budu u stanju da srazmerno koriste silu?“ „Hoće li AI moći da prepozna neprijateljske znakove predaje?“ „Ko će biti odgovoran za neopravdano robotsko ubistvo?“ „Kako se kodifikuje urođeno subjektivno tijelo etičkih standarda i praksi?“. Takva pitanja dovela su do toga da je nekoliko međunarodnih pokreta protiv „robot ubica“.⁵⁹

U julu 2015. godine, više od 1.000 istraživača robotike i vještačke inteligencije potpisalo je otvoreno pismo u kojem se poziva na zabranu ofanzivnog autonomnog oružja (sa potpisnicima više od 20 hiljada ljudi). I na posljednjoj Konvenciji Ujedinjenih nacija o konvencionalnom naoružanju, 123 zemlje učesnice glasale su da se sazove grupa vladinih stručnjaka kako bi se formalno pozabavilo pitanjem zakona o tom pitanju, što bi potencijalno moglo dovesti do međunarodne zabrane. Ishod ovih predstojećih sastanaka je neizvjestan, jasno je da političke, kulturne i osnovne dimenzije ljudskih prava u ovom pitanju tek počinju da se istražuju. Potrebno je obratiti pažnju na analizu operativnog uticaja koji svakako predstavlja ograničenje (ili direktnu zabranu) upotrebe ofanzivnog autonomnog oružja koje može imati za američke vojne snage.⁶⁰

⁵⁸ Sydney J. Freedberg, Jr. (2018), “Pentagon Rolls Out Major Cyber, AI Strategies This Summer,” *Breaking Defense*, July 17.

⁵⁹ Velez-Green, A., Scharre, P. (2017), “The United States Can Be a World Leader in AI. Here’s How.,” *The National Interest*, November 2.

⁶⁰ Sydney J. Freedberg, Jr. (2018), “Pentagon Rolls Out Major Cyber, AI Strategies This Summer,” *Breaking Defense*, July 17.

3.5.4. Prelaz na nova područja autonomije u vojsci

Ključni (međusobno isprepleteni) koraci prelaza na nova područja autonomije u vojsci uključuju:⁶¹

- Korak 1: Sprovođenje osnovnih AI istraživanja na više domena (zeleno-crveno preklapanje naglašavajući da su istraživanja u različitim AI oblastima, npr. duboko učenje, prepoznavanje slika i robotski rojevi nužno odvijaju se različitim brzinama i postoje, u bilo kom trenutku, na različitim nivoima sazrijevanja).
- Korak 2: Razumijevanje načina na koji pojedini AI istraživački domeni ulaze u bezbroj komponenti koje sačinjavaju autonomne sisteme, uključujući i njihovo povezivanje sa ljudskim operaterima (što dalje podrazumijeva razumejvanje kako ljudski-mašinski kolaborativni sistemi funkcionišu u specifičnim okruženjima misija).
- Korak 3: Premještanje dizajna, razvoja, testiranja i akreditacije kroz proces nabavke DOD-a (i prilagođavanje jedinstvenog skupa tehničkih izazova autonomije pri tome).
- Korak 4: Tumačenje i projektovanje potrebnih nivoa zrelosti sistemskih mogućnosti koje autonomni sistemi moraju imati za specifične misije.

⁶¹ Sydney J. Freedberg, Jr. (2018), "Pentagon Rolls Out Major Cyber, AI Strategies This Summer," *Breaking Defense*, July 17.

4. ZAKLJUČAK

Zaključujemo da su savremene tendencije u domenu vještačke inteligencije vezane za razvoj neuronskih mreža i unapređivanje ekspertnih sistema. Uloga ekspertskih sistema u ovom kontekstu je reprodukcija ljudskog razmišljanja preko specifičnih simbola pretvorenih u vještačku inteligenciju. Vještačka inteligencija kao pojam u širem smislu, označava kapacitet jedne vještačke tvorevine za realizovanje funkcija koje su karakteristika ljudskog razmišljanja. Definiciju vještačke inteligencije, odnosno pojam je prvi put predstavljen 1956. godine u Hanoveru u SAD, na simpozijumu istraživača koji su predstavljali teorije koje su vezane za inteligenciju, neuronske mreže i automate (robote).

U narednim godinama, koncept vještačke inteligencije se ubrzano usavršavao, a razvoj je danas u najvećem obimu, pa se istraživači širom svijeta utrkuju ko će napraviti najinteligentniju mašinu i da će vještačka inteligencija dostići imaginarnu granicu stvaranja robota koji će imati inteligenciju sličnu ili istu kao i čovjek („homo roboticus“). Mnogi AI programi su napravljeni da riješe neke korisne probleme bez obzira na njihove sličnosti sa ljudskom mentalnom arhitekturom. Čak i ekspertski sistemi, iako se u njihovom izvođenju koristi mnogo znanja stručnjaka, stvarno ne pokušavaju da simuliraju ljudsko unutrašnje rješavanje mentalnih procesa, sa aspekta rješavanja problema. Ako mentalna predstava predstavlja jedini kriterijum na kome će vještački sistem funkcionisati, onda možda postoji malo razloga da se pokušaju simulirati ljudske metode rješavanja problema; u stvari, programi koji kroz nehumane pristupe rješavaju probleme (primjer igre šaha, koju će računar skoro uvijek riješiti u svoju korist), pa računari često imaju više uspjeha nego njihove ljudske „kolege“.

Američka Nacionalna strategija odbrane, objavljena u januaru 2018. godine, identifikovala je vještačku inteligenciju kao jednu od ključnih tehnologija koja će osigurati Sjedinjenim Državama da se mogu boriti i pobijediti u ratovima. Američka vojska već integriše AI sisteme u borbu putem inicijative pod nazivom Project Maven, koja koristi AI algoritme za identifikaciju pobunjeničkih ciljeva u Iraku i Siriji.

Različita ministrastva i sektori u svijetu u modernom vremenu razmatraju niz različitih aplikacija za AI. Trenutno je istraživanje i razvoj AI prepušteno diskreciji istraživačkih organizacija u pojedinačnim službama, kao npr. DARPA (*Defense Advanced Research Projects Agency*) i Agencija za napredne istraživačke projekte (IARPA) u SAD. Očekuje se da će AI

biti posebno korisna za obavještajne podatke zbog velikih skupova podataka dostupnih za analizu. Na primjer, prva faza projekta Maven uključuje automatizaciju obrade obavještajnih podataka kao podršku protiv ISIL kampanji. Konkretno, Project Maven tim uključuje algoritme za kompjutersku viziju i računarsko učenje u inteligentne ćelije za prikupljanje koje bi češljale snimke iz nenaseljenih letilica i automatski identifikovane neprijateljske aktivnosti za ciljanje neprijateljskih lokacija širom svijeta.

AI može imati perspektivnu budućnost u oblasti vojne logistike. Vazduhoplovstvo, na primjer, počinje da koristi AI za predviđanje održavanja aviona. Umjesto popravke kada se avion slomi ili u skladu sa monolitnim planovima održavanja flote, vazduhoplovstvo testira AI-pristup koji prilagođava rasporede održavanja potrebama pojedinačnih aviona. Ovaj pristup, koji se trenutno koristi u Automatizovanom logističkom informacionom sistemu F-35, izvlači podatke senzora u realnom vremenu ugrađene u motore aviona i druge sisteme na brodu i unosi podatke u algoritam predviđanja kako bi odredio kada tehničari trebaju pregledati avion ili zamijeniti dijelove. Američka vojska npr. nastoji da iskoristi analitički potencijal AI u oblasti komandovanja i kontrole. Vazduhoplovne snage razvijaju sistem za višenamjensko komandovanje i kontrolu (MDC2), koji ima za cilj da centralizuje planiranje i izvođenje vazdušnih, svemirskih, kibernetičkih, morskih i kopnenih operacija. U bliskoj budućnosti, AI se može koristiti za spajanje podataka sa senzora u svim ovim domenima da bi se stvorio jedan izvor informacija, poznat i kao „zajednička operativna slika“, za donosiocima odluka. Trenutno, informacije koje su na raspolaganju donosiocima odluka dolaze u različitim oblicima formata sa više platformi, često sa viškom ili nerješanim neusaglašenjima.

5. LITERATURA

1. Allen G., Chan, T. (2017), *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs.
2. Campbell, M. (2015), "Knowledge discovery in Deep Blue," *Comm. of the ACM* 42, Nov.
3. Clark, C. (2017), "Our Artificial Intelligence 'Sputnik Moment' is Now: Eric Schmidt and Bob Work," *Breaking Defense*, November 1.
4. Corrigan, J. (2018), "U.S. Needs a National Strategy for Artificial Intelligence, Lawmakers and Experts Say," *Defense One*, July 14.
5. Department of Defense (2017), *Joint Concept for Robotic and Autonomous Systems*.
6. Ilachinski, A. (2017), *AI, Robots, and Swarms, Issues, Questions, and Recommended Studies*, Center for Naval Analysis, January.
7. Ilić, V. (1999), *Veštačka inteligencija*, Beograd: SOLAIR.
8. Janičić, P., Nikolić, M. (2017), *Veštačka inteligencija*, Beograd: Matematički fakultet Univerziteta u Beogradu.
9. Koch, C. (2016), "How the Computer Beat the Go Master," *Scientific American*, 19 March.
10. Luger, G. (2007), *Artificial intelligence*, sixth edition, Boston: University of New Mexico.
11. McKinsey Global Institute (2017), *Artificial Intelligence, The Next Digital Frontier?*, June.
12. Mills, S. (2017), Presentation at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7.
13. Scharre, P. (2015), Horowitz, M., *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February.
14. Schmidhuber, J. (2014), "Deep Learning in Neural Networks: An Overview," *Technical Report IDSIA-03-14*, arXiv:1404.7828 v4.
15. Sydney J. Freedberg, Jr. (2018), "Pentagon Rolls Out Major Cyber, AI Strategies This Summer," *Breaking Defense*, July 17.
16. U.S. Congress (2018), House of Representatives Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies*, 115th Cong., 2nd sess., January 9.

17. Velez-Green, A., Scharre, P. (2017), “The United States Can Be a World Leader in AI. Here’s How.,” *TheNational Interest*, November 2.
18. Weisgerber, M. (2017), “The Pentagon’s New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS”, *Defense One*, May 14.
19. <http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-itsfirst-mission-hunt-isis/137833/> (27.3.2019.)
20. <https://www.army.mil/e2/c/images/2014/05/05/343431/size0.jpg> (27.3.2019.)
21. <https://cdn.mainichi.jp/vol1/2016/08/26/20160826p2a00m0na020000p9.jpg?1> (27.3.2019.)
22. <https://thedefensepost.com/wp-content/uploads/2017/11/defender-autonomous-robot-081118-F-1025B-001-1170x610.jpg> (25.3.2019.)
23. <https://www.acq.osd.mil/dsb/reports/2010s/DSBSS15.pdf> (23.3.2019.)
24. <https://breakingdefense.com/2017/11/our-artificial-intelligence-sputnik-moment-is-noweric-schmidt-bob-work/> (22.3.2019.)
25. <https://www.darpa.mil/attachments/AIFull.pdf> (29.3.2019.)
26. <https://www.darpa.mil/attachments/AIFull.pdf> (27.3.2019.)
27. <https://www.defenseone.com/technology/2018/07/us-needs-national-strategy-artificial-intelligencelawmakers-and-experts-say/149644/> (21.3.2019.)
28. <https://breakingdefense.com/2018/07/pentagon-rolls-out-major-cyber-ai-strategies-this-summer/> (19.3.2019.)