DOI: 10.5937/vojdelo1803236M

VELIKE BAZE PODATAKA – *BIG DATA*, PRIMENA U VOJNO-BEZBEDNOSNOM SISTEMU

Žarko Milojević*
Univerzitet Hohenhajm, Ekonomski Fakultet
Ljubomir Dulović
Generalštab Vojske Srbije, Uprava za planiranje i razvoj

Aktuelni bezbednosni izazovi razvijenih zemalja su kontrola granica; ilegalni protok ljudi, oružja i novca; sajber terorizam; islamski radikalizam. Upotreba i analiza velikih količina podataka – *Big Data* doprinosi preciznijem identifikovanju faktora relevantnih u procesu donošenja odluka u mnogim sferama. Efikasno praćenje kretanja pojedinaca, potpunije predviđanje postupaka subjekata, sprečavanju neželjenih aktivnosti useljenika u zemlji domaćina je takođe domen primene. Savremena vojna oprema podrazumeva manipulaciju voluminoznim podacima. Domen primene *Big Data* jeste osnovni istraživački cilj rada.

Autori dodatno ukazuju na problem kompleksnosti akumulacije podataka; volumen evidencije kriminalno-terorističkih elemenata; efektivnost rada službi bezbednosti u oblasti sajber aktivnosti kao i efikasnost rada vojnih organa. Stručni rad elaborira signifikantnost *Big Data* u efikasnosti vojnih dejstava, praćenja inostranih visoko tehnoloških aktivnosti, primene u vojnim operacijama. Istraživački rad je zasnovan na kvalitativnoj metodi. Predmet analize je način korišćenja i primena velikih količina podataka u bezbednosnim strukturama industrijski razvijenih zemalja. Opis stepena i obima aplikacije voluminoznih podataka u odbrambenom sistemu zemlje je poseban doprinos rada. Nalazi upućuju na relevantnost velikih količina podataka u namenskoj industriji. Istovremeno, zaključci upućuju na značaj *Big Data* u podizanju nivoa nacionalne sigurnosti i međuinstitucionalnom procesuiranju podataka u sajber-prostoru i obaveštajnim aktivnostima. Rezultati sprovedene analize su od važnosti za vojno-bezbednosne strukture u zemlji kao i za državni administrativni aparat.

Ključne reči: *Big Data, administracija podataka, vojna informaciona tehnologija, vojno-bezbednosne službe, sajber terorizam*

Uvod

Razvoj informacionih tehnologija i interneta je znatno unapredio generisanje vanredno velikog obima podataka i informacija[1] koje su često nestrukturirane, kao što su: sadržaji na društvenim medijima (*Facebook, Twitter, You Tube*, *Instagram, Linke-*

* zarko_milojevic@uni-hohenheim.de

[1] Studije sprovedene na Univerzitetu Berkli 1999. i 2003. govore da se u svetu generiše oko 1,5 milijardi gigabajta (GB) informacija na godišnjem novou, dok se taj broj do 2003. udvostručio.

dIn); državna administracija (biometrijski podaci građana); naučna istraživanja (Hadronski kolajder u *CERN*-u, projekat *SDSS* u astronomiji); poslovne aktivnosti (industrija, bankarstvo, logistika); namenska industrija (kontrola bespilotnih letelica – *UAV*, projekat *RAPIER*, projekat *MUSE*); internet prodaja (*eBay*, *Amazon*); satelitska navigacija u saobraćaju; imejl korespodencija; mobilni telefoni, itd. Postavljaju se pitanja: Kako pristupiti analizi podataka čiji je volumen drastično veći od tradicionalnog i kakve instrumente koristiti radi ekstrapolacije rezultata? Na koji način zaštititi osetljive podatke o građanima, institucijama, Vladama? Može li se ostvariti efikasnija upotreba vojnih resursa u operacijama upotrebom velikih baza podataka?

Analizom izuzetno velikih količina informacija (eng. *Big Data*) omogućava se predviđanje ishoda događaja, procesa, posebno ljudskog ponašanja, a na osnovu otkrivanja šablona, trendova, veza i interakcija između faktora. Time se pospešuje proces donošenja odluka, otkrivaju prevare i pretnje, pronalaze novi izvori prihoda, stvaraju patenti i invencije, usavršavaju operacije i procesi, generišu nove informacije. Popularni društveni mediji osim razmene i akumulacije biometrijskih podataka, mogu poslužiti i kao sredstvo za zloupotrebu istih.[2] Problem visoko tehnološkog kriminala i sajber terorizma su poseban aspekt svakodnevice. Implementacijom informacionih sistema i *Big Data* u namenskoj industriji postižu se viši standardi u eksploataciji namenskog naoružanja i uvećava se stepen uspešnosti realizacije u vojnim operacijama.[3]

Definicija i domen *Big Data*a i *Big Data* analitike

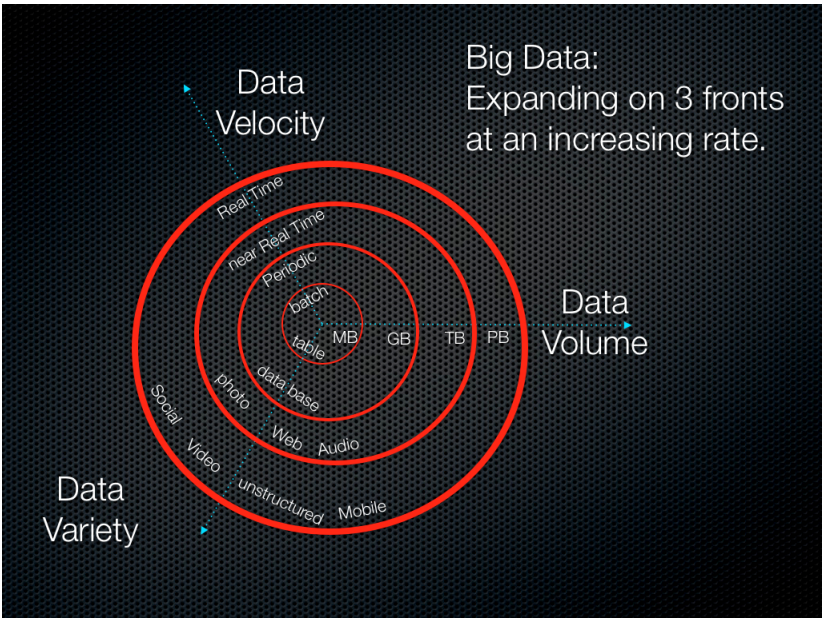
Pojam *Big Data*[4] (srp. veliki podaci; velike baze podataka, voluminozni podaci) jeste sistem zasnovan na određenoj informacionoj tehnologiji. Odnosi se na količinski obimne strukturisane ili nestrukturisane podatke. Služi da označi velike skupove podataka čiji volumen prevazilazi tradicionalne načine skladištenja. Pretraživanje na *Google* daje 275 miliona nalaza "Big Data" u 2017, od čega 25,8 miliona čine vesti, 53,3 miliona čine video zapisi a 760.000 broje knjige; 35,9 % ukupnih nalaza je izdato na prostoru SAD-a; u periodu od 01.01.2000. do 31.12.2011. objavljeno je 93,2 miliona podataka dok je u periodu od 01.01.2012. do 10.04.2017. uneto 741 milion podataka; u prethodnih 60 minuta u odnosu na vreme pretrage objavljeno je 15.100 podataka; istovetnom pretragom na *Google Scholar* dobija se ukupnih 4,58 miliona nalaza gde 1,75 miliona broje nalazi izdati u periodu od 2000. do 2010. Može se zaključiti da je termin *Big Data* relativno novijeg datuma i da je predmet pažnje auditorijuma.

[2] Sudski procesi protiv Edvarda Snoudena i Džulijana Ansanža; Usvajanje zakona o nadgledanju (Velika Britanija – *Investigatory Powers Act* 2016, Francuska – *Loi n° 2015-912 du 24 juillet 2015 relative au renseignement* 2015).

[3] Više informacija dostupno u radovima Couch, N. & Robins, B. (2013); Song et al. (2015).

[4] Sam naziv je prvi put upotrebljen u radu Michael Cox (1997), zatim javno korišćen (John Mashey, 1998) od strane načelnika istraživačkog odeljenja u firmi Silicon Graphics. Kasnije bliže određenje je dato (Dough Laney, 2001). Hronološki prikaz upotrebe izraza Big Data videti u radu Gu & Zhang (2014, pp. 815-816). Sažet izveštaj o definicijama pojma videti u Forbes 2014. Idejno rešenje primene Big Data dolazi od korporacije Google stvaranjem GFS (2003) i MapReduce (2004). Učestalost korišćenja pojma raste tek od nedavno – 2011 (Gandomi & Haider, 2015, p. 139).

Fenomen velikih baza podataka – *Big Data*, karakterišu: obim (eng. *volume*), raznovrsnost (eng. *variety*), brzina opticaja (eng. *velocity*), pouzdanost (eng. *veracity*), neizvesnost (eng. *verocity*), složenost (eng. *complexity*), verovatnost (eng. *probability*), osetljivost (eng. *sensibility*), kvalitet (eng. *quality*), vrednost (eng. *value*).[5]



Slika 1 – *Grafički prikaz osnovnih dimenzija Big Data*
(Izvor: http://api.ning.com/files/O6-JQcfS6sxRuZ8I2i5nJVa59xL-krT-a6UqeoLNaHwL2w-JSR-Cy56PmikOywRQgy2gDf YxLAb0Hs*VFr8IePv5QFBJdhDH/BigData.001.jpg)

Podaci koji se skladište a karakterišu se kao voluminozni, svojim obimom prevazilaze kapacitete komercijalnih skladišnih uređaja.[6] Za generisanje takvih tipova podataka, uprošćeno rečeno, koristi se informaciona tehnologija zasnovana na:

– Hardveru – serveri i oblaci znatnog kapaciteta koji imaju funkciju centralne jedinice na koju se skladište podaci,

– Softveru – alati i aplikacije kojima se uneti objekti povezuju sa serverom (npr. Hadoop, NoSQL, MapReduce, InfoSphere, BigInsights, Internet of Things),[7]

– objektima koji šalju informacije serveru (npr. GPRS na mobilnim telefonima, RFID identifikacija poslatih pošiljaka, očitavanja senzora, snimci video kamera...).

[5] Pogledati kod META Group (2001); Oracle Corp. (2013, p.3); IBM Corp. (2014); Gezy (2014); IBM Corp. (2015, p. 5); Hilbert (2015), SAS (2015).

[6] Kapacitet skladištenih podataka se meri u petabajtima i eksabajtima u samo jednom skupu podataka. Sistematizaciju mernih jedinica za skladištenje podataka videti u izveštaju IBM (2015, pp. 5-6). Američki lanac prodajnih centara Walmart sakuplja 2,5 petabajta po satu od transakcija svojih mušterija (Mc Afee & Brynjolfsson, 2012).

[7] Više informacija o arhitekturi platforme za akumulaciju velikih baza podataka može se videti kod Apache (2017); Oracle Corp. (2016, pp. 18-22); Intel IT Center (2015, p.8); IBM Corp. (2011).

Podela podataka se može izvršiti prema osam osnovnih kriterijuma: vrsta analize, način stvaranja, učestalost stvaranja, vrsta, sadržaj, izvori, ciljna grupa i upotrebljeni hardver. Ilustracija primene *Big Data*: predviđanje kućne potrošnje, analiza ponašanja klijenata u telekomunikacijama, promocija u maloprodaji kod potrošača na osnovu njihove lokacije u gradu, sprečavanje pronevera u bankarstvu i zdravstvu (lažne kartice), personalizovanje ponude u maloprodaji na osnovu prepoznavanja lica potrošača i njihovog ponašanja na društvenim mrežama i sl.[8] Akumuliranje podataka međutim, ne pruža doprinos donosiocu odluka bez analitike kao komplementarnog procesa.

Big Data analitika

Sintagma *Big Data Analytics* (srp. analitika velikih baza podataka) predstavlja analiziranje, predviđanje odnosno inteligentno donošenje odluka na osnovu prikupljenih podataka.[9] Termini *Big Data* i *Big Data Analytics* nisu isključivi i formiraju jednu komplementarnu celinu.

Analitika voluminoznih podataka jeste postupak predviđanja ponašanja objekata ili uočavanja trendova na osnovu serija prikupljenih (ne)strukturiranih podatka. Čini sastavni deo industrijskih operacija u mnogim privrednim granama (maloprodaja, veleprodaja, zdravstvo, bankarstvo, osiguranje, tržište kapitala – berze, transport, *inter alia.*[10] U periodu od 2016. do 2020. doći će do porasta prihoda u industrijskim sektorima gde se pružaju usluge *Big Data* i poslovne analitike; visina prihoda u 2016. je iznosila 130,1 milijardi $ na svetskom nivou dok je za 2020. projektovano 203 milijarde $. Katalizatori predviđenog rasta u prihodima su: dostupnost podataka, tehnologija nove generacije i trend donošenja odluka zasnovanog na akumuliranim podacima. Industrijski sektori bankarstvo, pojedinačna proizvodnja, serijska proizvodnja, javni sektor, te profesionalne usluge čine 50% predviđenog porasta prihoda od korišćenja *Big Data*. Upravljanje rizikom, sprečavanje pronevera i usaglašavanje poslovnih aktivnosti čine osnovicu upotrebe voluminoznih podataka u bankarstvu. Telekomunikacioni, uslužni, osiguravajući i transportni sektor biće pokretači predviđenog rasta prihoda pored prethodno pomenutih. Velike kompanije (više od 1.000 zaposlenih) su osnovni pokretač ulaganja u *Big Data* i analitiku. Visina njihovih ulaganja u 2018. je projektovana na nivou od 100 milijardi $. Male i srednje firme čine četvrtinu projektovanog rasta u prihodima velikih firmi. Više od polovine svih predviđenih prihoda biće na teritoriji SAD-a, zatim sledi Zapadna Evropa.[11] Posledično, kompanije sa značajnim učešćem na tržištu softvera za naprednu i prediktivnu analitiku jesu američke poput SAS, IBM, Microsoft.[12] Segment industrije pružanja usluga korišćenja volumino-

[8] Šematski prikaz videti kod Mysore et al. (2013). Pomenute su samo neke od primena.

[9] Njujorška policija vrši predviđanja novih mesta krivičnih prestupa na osnovu istorijskih podataka o kriminalnim deliktima uparenim sa gustinom saobraćaja, sportskim dešavanjima, isplatama dohodaka i sl. (Rayport, 2012). Sticanje osetljivih ličnih podataka na osnovu aktivnosti na društvenim mrežama je izvodljivo upotrebom instrumenata i Big Data. (Kosinski *et al.*, 2013).

[10] Vrlo sažet tekst o relevantnosti Big Data i isplativosti upotrebe Big Data analitike može se naći kod Forbes (2016).

[11] Više informacija dostupno u izeštaju IDC Corp. (2017).

[12] Potpuna lista kompanija sa najvećim tržišnim učešćem i prihodima u periodu 2013-2015 dostupna je u izveštaju Vesset *et al.* (2016, p. 5).

znih podataka i analitike se nalazi u ekspanziji.[13] Među krajnjim korisnicima usluga pruženih u ovom segmentu industrije su državne i javne institucije.[14] Rezultati istraživanja u 2015. beleže uvećanje poslovnog značaja voluminoznih podataka i na njima primenjene analitike kod kompanija srednje veličine (500 zaposlenih) i velikih kompanija (više od 1.000 zaposlenih). Dodatno, uprava ispitanih kompanija ocenjuje *Big Data* analitiku kao bitan element sticanja konkurentske prednosti. Trećina podataka vezanih za određivanje lokacije se generiše korišćenjem *Big Data*.[15]

Postupak analiziranja-analitike se koceptualno deli na dve celine: oblikovanje/modeliranje uz analizu; interpretacija.[16] To su zapravo tehnike kojima se stiče iskustvo i pamet na osnovu velikih baza podataka. Među osnovnim tehnikama *Big Data* analitike mogu se izdvojiti:[17]

a) analitika teksta – dobijanje informacija iz napisa u društvenim medijima, e-pošti, blogovima, onlajn forumima, poslovnim dokumentima, vestima, odgovorima na upitnike, razgovorima u pozivnim centrima. U upotrebi su tehnike poput algoritamske ekstrakcije podataka, konciznog sumiranja teksta, servisa za odgovore na pitanja (npr. Siri i Watson), ispitivanje stavova;

b) audio analitika – prikupljanje informacija iz snimljenih razgovora (npr. pozivni centri kompanija, bolničko dijagnostikovanje mentalnih poremećaja ili utvrđivanje stanja novorođenčadi na osnovu boje, visine i jačine glasa);

v) video analitika – generisanje informacija na osnovu video sadržaja (npr. sigurnosno nadgledanje objekata, prisluškivanje, ispitivanje ponašanja kupaca u maloprodajnim lancima);

g) analitika društvenih medija – sticanje informacija na osnovu podataka objavljenim na društvenim medijima[18] (npr. identifikovanje zajednica/komuna, društveni uticaj natpisa na pojedince, uzajamna povezanost entiteta na medijima);

d) predviđanje – donošenje odluka na osnovu prikupljenih i obrađenih podataka i iz njih izvedenih informacija upotrebom prevashodno statističkih tehnika poput kretanja prosečnih vrednosti i linearna regresija (npr. predviđanje sledeće kupovine potrošača, predviđanje pada aviona).

Upotreba velikih baza podataka u vojne svrhe

Izdvajanja za Big Data analitiku u okviru vojne industrije

Sticanje prednosti na osnovu upotrebe *Big Data* analitike ima visok prioritet za vojne snage. To je posledica rasta upotrebe sistema bez ljudske posade, oslanjanja na obaveštajne, prislušne i izviđačke tehnologije. Pomenutim rastom upotrebe takvih sredstava opterećuje se

[13] Relativno sažet i sveobuhvatan prikaz kompanija čije je poslovanje vezano za Big Data i analitiku, može se videti kod Turck (2016). Dodatna lista kompanija dostupna je na http://dfkoz.com/big-data-landscape/

[14] Stratistics (2016), dostupno na http://www.strategymrc.com/report/big-data-analytics-hadoop-market

[15] Dostupno u izveštaju International Institute for Analytics (2016, pp. 18-20).

[16] Za dodatno objašnjenje pogledati izlaganje Labrinidis & Jagadish (2012, p. 2032).

[17] Više informacija dostupno u radu Gandomi & Haider (2015, pp. 140-143).

[18] Zanimljivu klasifikaciju tipičnih potkategorija društvenih medija dali su u svojim radovima Gundecha & Liu (2014, p. 3); Barbier & Liu (2011, p. 330).

delovanje vojnika na terenu i civila zaposlenih u sektoru odbrane jer se akumulira veliki broj podataka za obradu. Brza obrada podataka i razvijanje instrumenata analize treba biti u funkciji omogućavanja vojnicima na terenu da primaju obaveštajne podatke.[19] Osoben problem je i dostupnost stručnjaka sposobnih da analiziraju veliku količinu podataka, a zatim na osnovu svojih veština i radnog iskustva pravilno protumače različite vrste složenih struktura podataka. Tu se zapravo ogleda značaj primene algoritama i *Big Data* kompjuterizovanih instrumenata čijom se primenom stvara dovoljan broj informacija zadovoljavajućeg kvaliteta.[20]

Najveća izdvajanja u 2015. godini za namensku industriju i vojni sektor imaju SAD čija visina budžeta predstavlja zbir narednih 8 država na listi. Budžet američkog ministarstva odbrane u fiskalnoj 2017. godini predviđa 12,5 milijardi $ ulaganja samo u nove tehnologije. Ukupno izdvajanje za istraživanje, razvoj, testiranje i evaluaciju iznosi 71,8 milijardi $. Pored izdvajanja za podršku operacijama, vazdušne snage, mornaricu, raketno i pešadijsko naoružanje, ulaganje u nauku i tehnologiju predstavlja bitnu stavku u budžetu odbrane za 2017, mereći visinu izdvojenih sredstava. Uz kosmičke sisteme i odbrambeni raketni program, operacije u sajber[21] prostoru kao i nauka i tehnologija, čine ključne inicijative predviđene američkim budžetom odbrane.[22] Među 20 najunosnijih tendera raspisanih na saveznom nivou u 2016. godini, nešto više od polovine su tenderi raspisani za ministarstvo odbrane i vojnih snaga Amerike, od toga 65% sačinjavaju tenderi vezani za informacione tehnologije.[23] Obim ulaganja u *Big Data* analitiku u Agenciji za napredne istraživačke projekte odbrane (eng. Defence Advanced Research Project Agency) u 2016. je bio na nivou od 82,3%[24] ukupnog budžeta Agencije koji je iznosio 2,87 milijardi $. Praćenje aktivnosti dobavljača Ministarstva odbrane, skladištenje podata vojnih operacija, nadzor nad inicijativama službenika predstavlja srž platforme za voluminozne podatke u okviru analitičkog odeljenja američke agencije za informacione sisteme koja se nalazi u okviru hijerarhije Ministarstva odbrane (eng. Defence Information System Agency). U dodatne funkcije spada sledeće: sprovođenje agregacije podataka, korelacija podataka, ekstrapolacija trenda prema istorijskim podacima, forenzička analiza strukturiranih i nestrukturiranih podataka. Pristup platformi imaju vojske zemalja partnera u okviru NATO.

Ministarstvo odbrane Ujedinjenog Kraljevstva (UK) je u 2016. predstavilo plan o ulaganju 40 miliona funti za izgradnju novog operativnog centra za sajber odbranu. Sajber bezbednost je označena kao prioritetna aktivnost. Planirano je nešto manje od 2 milijarde funti alociranih sredstava u narednih pet godina za elektronsko obaveštavanje i nadgledanje. *Big Data* analitika je prema izjavi britanskog načelnika sajber odbrane označenja kao „vrhunska prednost".[25] UK je u periodu od 2014. do 2015. godine najviše izdvaja-

[19] Više informacija dostupno u radu Young (2012).

[20] Mišljenje dr. Eric Little potpredsednika i glavnog naučnog radnika kompanije Modus Operandi, dobavljača američkih kopnenih snaga.

[21] Termin „sajber" označava internet ili elektronski zasnovanu aktivnost. Prevashodno se odnosi na aktivnosti elektronskih napada na sajtove, preuzimanje osetljivih podataka sa servera i sl.

[22] Više informacija se može naći u pregledu američkog budžeta za odbranu Defence budget overview (2017, p. 46).

[23] Detaljan prikaz poslovnih poduhvata, vrednosti ugovora i kupaca dostupno u izveštaju Deltek (2015, pp. 8-10).

[24] Na portalu tehničkog informacionog centra (eng. Defence Technical Information Center) koji je registrovan kao agencija u okviru Ministarstva odbrane SAD-a, koristeći filtere može se dobiti lista odobrenih projekata sa specifikacijama za svaku fiskalnu godinu počevši od 2000. godine.

[25] Dostupno na Financial Times (2016).

lo za namensku industriju i vojsku u okviru Evropske Unije (EU) sa prosečnih 50 milijardi evra. Slede Francuska i SR Nemačka respektivno. Pomenute zemlje najviše ulažu u vojna istraživanja i razvoj sa 3,75 milijardi € (7,8% ukupnog vojnog budžeta); 3,56 milijardi € (9,1% ukupnog vojnog budžeta) i 0,84 milijardi € (2,4% ukupnog vojnog budžeta) respektivno.[26] Pod okriljem Evropske agencije za odbranu (eng. European Defence Agency) registrovano je ukupno 25 projekata u 2016. u oblasti vojnog istraživanja i razvoja ukupne vrednosti od 120 miliona €.[27]

Primena Big Data u vojnom sektoru

Tehnološki napredak u oblasti analitike voluminoznih podataka je označen kao jedan od glavnih faktora konkurentnosti proizvođača naoružanja u namenskoj industriji.[28] Širok spektar upotrebe velikih baza podataka se ogleda u sledećim vojno-organizacijskim podsistemima:

– vazduhoplovne jedinice;
– sajber-bezbednost;
– komandovanje/kontrola/komunikacija/obaveštavanje/nadgledanje/izviđanje;[29]
– podsistem raketnog navođenja,
– pomorski podsistemi,
– podsistem radara i senzora,
– obuke personala.

Američka mornarica razvija program *NTCRI* čiji je cilj dostupnost velikog broja kvalitetnih informacija u toku operacija na taktičkom nivou.[30] Projekat *ARCYBER* služi podsticanju elektronskih dejstava u defanzivnim i ofanzivnim operacijama u sajber prostoru i zaštiti elektronske nacionalne bezbednosti od taktičkog do strateškog nivoa.[31] Predviđanje postupaka neprijateljske strane se unapređuje primenom voluminoznih podataka.[32] Kineski vojni vrh preispituje sposobnost skrivanja svog pokretnog sistema interkontinentalnih balističkih raketa usled kompjuterskog napretka američkog načina izviđanja zasnovanog na analitici voluminoznih podataka.[33] Zemaljski sistem nadgledanja *ARGUS* generiše više od 40 GB informacija u sekundi.[34] Sa takvom infrastrukturom moguće je u približno realnom vremenu crpeti relevantne informacije iz dostupnih podataka čime se smanjuju rizici pri odlučivanju. U svom radu Yang *et al.* (2016) dokazuju da se

[26] Za kompletan uvid pogledati izveštaj Guzelyte (2016, p. 31,33).

[27] Pročitati godišnji izveštaj agencije – European Defence Agency, Annual Report (2016, p. 26).

[28] Godišnji izveštaj korporacije Lockheed Martin za 2016, str. 7.

[29] Istorijski osvrt i analiza podsistema data je u radu Starr (2003). Konkretni primeri datog podsistema: balističko-raketni odbrambeni sistemi poput AEGIS i DIAMOND; centar za vazdušna osmatranja i izviđanje, modeli letelica P-3 Orion, U-2 Dragon Lady, Aerostat 74K-420K-56K.

[30] Vrednost poslovnog poduhvata je 400.000 $, rok završetka je 11 meseci sa mogućnošću produženja. Pročitati više na https://www.cra.com/company/news/office-naval-research-enlists-charles-river-analytics-navy-tactical-cloud

[31] Informacije dostupne na http://www.arcyber.army.mil/Pages/ArmyCyber.aspx

[32] U naučnom radu (Kim et al, 2017, p. 14) autori pružaju statističke argumente o poboljšanju modela predviđanja postupaka vlasti u Severnoj Koreji pri upotrebi Big Data za 47%.

[33] Više dostupno u članku MacDonald & Ferguson (2015).

[34] Više dostupno u izveštaju ROSI (2013) na https://www.rusi.org/downloads/assets/RUSI_BIGDATA_Report_2013.pdf

pri upotrebi adaptivnog genetičkog algoritma, kao instrumenta *Big Data* analitike, pospešuje efikasnost dejstava na bojnom polju za 37% mereno prema situaciji bez primene *Big Data* analitike.[35] Navedeno poboljšanje je vezano za brzinu identifikacije tipa, mesta i jačine naoružanja neprijateljskih pozicija na osnovu video snimaka u istom trenutku opažanja, te zatim dejstvo na iste nakon relativno kraćeg vremenskog intervala. Algoritmom se na osnovu preuzetih podataka utvrđuju faktori rizika – naoružanje neprijatelja/letelice/objekta/vozila, i kompjuterskom analizom daju predlozi odluke protiv dejstava. Efikasnost *Big Data* analitike korišćenjem slične metodologije je potvrđena i kod identifikacije neregistrovanih vozila u Šangaju (Xu *et al.* 2015, pp. 223-224). Predviđanje zasnovano na analizi video snimaka je naročito važno u vazdušnim dejstvima gde je bitno utvrditi tip naoružanja neprijateljskog objekta. Izraelske vojne snage od 2013. u svom sastavu imaju jedinicu za tehnologiju Macpen (eng. Matzpen), čiji je zadatak razvitak i stvaranje softverskih komponenti. Rezultat su sistemi poput Kristalne kugle (eng. Crystal Ball) – prikupljanje i svođenje velikog obima podataka iz raznih izvora omogućavajući vojnim starešinama izbor informacija za dalju analizu; Cajad (eng. Tzayad) – direktna GPS komunikacija sa vojnicima na bojnom polju dozvoljava starešinama da znaju tačnu lokaciju vojnika, karakteristike reljefa, uslove okruženja. Time se donošenje odluka koje se tiču raspoređivanja jedinica, ili važnije načina kako poboljšati njihovu taktičku poziciju u toku same operacije. Dodatno, poboljšanje u logističkim manevrima tokom rata, to jest prevoz vojnika, opreme, sredstava, hrane. Softverska rešenja jedinice Macpen omogućila su regrutaciju, opremanje i slanje sredstava i vojnika u rat u vremenskom intervalu od nekoliko sati tokom rata protiv Hamasa u leto 2014.[36]

Tokom jednog celog dana misije jednostavne složenosti, bespilotna letelica dostavlja centrali 10 terabajta (TB) podataka od čega je samo 5% predmet analize dok se ostatak skladišti.[37] Nepostojanje uslova za analizu preostalog dela od 95% podataka minimizuje ukupan kvalitet donetih odluka na taktičkom nivou odlučivanja. Kvalitetna video veza, slanje fotografija visoke rezolucije, prenos tekstualnih sadržaja poput koordinata, očitavanja senzora itd. zajedno sačinjavaju tako veliki kapacitet transmisije. Bespilotna letelica prikuplja video-audio podatke u toku leta i pri nailasku na neprijateljske objekte ili jedinice preko video snimka dolazi do algoritamskog „isčitavanja" čime se identifikuje vrsta naoružanja, brojnost i položaj neprijatelja, te prosleđuje predlog rešenja komandnoj jedinici na osnovu analiziranih faktora rizika. Istovremeno, oslanjanjem na *Big Data* analitička rešenja povećava se sigurnost pilota u toku naleta usled poboljšanog predviđanja rizika u toku samog leta. Potrošnja goriva aviona i letelica biva smanjena. Utrošak vremenskih jedinica rada inženjera pri remontu aviona se umanjuje.[38] Oslanjanjem na velike baze podataka omogućava se prelazak sa periodičnog pregleda ispravnosti aviona na „uslovljeno održavanje", odnosno prema parametru. Takvim sistemom se u američkoj vojsci štedi 1,5 miliona $ godišnje.[39]

[35] Model predstavljen u radu Yang et al. (2016, p. 1364).

[36] Infromacije date od strane pukovnika Avner Ziva, načelnika Macpena. Za više informacija pogledati http://www.timesofisrael.com/winning-the-war-with-big-data/

[37] Videti više kod Kulshrestha (2016, r.4). Prema Fahey (2012), dron MQ-9 Reaper/Predator B je opremljen senzorima sa 12 kamera prečnika 4 kilometra efektivnog dometa; kapacitet generisanja informacija u toku jednog naleta se procenjuje na 4 terabajta (TB).

[38] Pročitati više kod Hooijdonk (2015) na https://www.richardvanhooijdonk.com/en/future-airforces-big-data/

[39] Saopštenje dato na godišnjoj konferenciji kompanije Teradata koja je u 2015. realizovala projekat za američke vazdušne snage. Više detalja dostupno na http://www.intelligent-aerospace.com/articles/2016/09/u-s-air-force-harnesses-data-management-and-analytics-platforms-to-enhance-aircraft-mro.html

Troškovi grejanja, električne energije u smeštajnim vojnim kapacitetima se smanjuju efikasnim nadgledanjem zasnovanim na *Big Data* upotrebi. Operativni troškovi vojnog osoblja opadaju upotrebom analitike velikih baza podataka.[40] Prijem novih pripadnika vojnih snaga je bitan element kvaliteta vojnog personala. Instrumenti analitike voluminoznih podataka (poput Google Trends, Google AdWords i Google Correlate) pružaju slojeviti uvid u promene stavova građanstva (naročito mlađe populacije) o vojsci tokom vremena; približavaju oglašavanje civilnih i vojnih radnih mesta onima koji na internetu pretražuju moguća zaposlenja u vojnom sektoru prema načinu njihove pretrage; moguće je predvideti šta je kandidat pretraživao na internetu nekoliko meseci pre nego što se prijavi za rad u vojsci. Time se poboljšava proces oglašavanja vojnih institucija u medijskom prostoru, privlače kandidati za prijem i predviđaju namere i htenja dela populacije zainteresovanog za prijem u vojnu službu.[41] Redukcija administrativnih troškova obrade i čuvanja podataka o celokupnom vojnom personalu se obezbeđuje stvaranjem velikih baza podataka i primenom napredne analitike – primer je *PDE* projekat američke vojske. Medicinski kartoni, rezultati psiholoških testova, disciplinskih prekršaja, ocene rada u službi zaposlenih u ministarstvu odbrane uključujući sve vojne rodove, porodica zaposlenih vojnih i penzionisanih vojnih lica kao i njihovih porodica, svi podaci se skladište na jednom repozitorijumu.[42] Dokumentovana međupovezanost i međuprenos biomedicinskih baza podataka, strukturna složenost podataka takvih arhiva, mogućnost audio vizuelnog skladištenja ekstenzivnih unosa, omogućava analitički uvid i arhiviranje informacija od značaja.[43] To je naročito od koristi ABHO centrima u razvijanju biološkog oružja.

Big Data u kontekstu rada obaveštajnih službi

Zakonska ovlašćenja o korišćenju podataka

Britanski parlament je krajem 2016. godine usvojio zakon (eng. Investigatory Powers Bill[44]) kojim se pravno dozvoljava obaveštajnim agencijama da presreću, preuzimaju, kontrolišu komunikaciju građana putem mobilne i fiksne telefonije. Celokupni protok podataka građana koje poseduju telekomunikacione kompanije je pravno obavezujuće ustupiti na korišćenje obaveštajnim i kontra-obaveštajnim agencijama u Britaniji.

Francuske vlasti su u julu 2015. usvojile zakon (fra. LOI n° 2015-912[45]) kojim se bez dozvole nadležnog suda pravno dozvoljava obaveštajnim službama da prikupljaju i prate komunikacioni protok podataka svojih građana. Time se podaci internet telefonskog saobraćaja stavlja na ustupanje vlastima bez posebne dozvole suda.

[40] U saopštenju ministra odbrane Republike Južne Koreje datom 2. februara 2017, operativni troškovi u 2016. godini su umanjeni za okvirno 22 miliona $ oslanjanjem na Big Data analitiku. Poboljšanje sigurnosti pilota u toku vojnih naleta je takođe navedeno u izjavi. Videti više na:
http://english.yonhapnews.co.kr/news/2017/02/07/0200000000AEN20170207003900315.html

[41] Detaljno objašnjenje sprovedene analize dostupno kod Jahedi *et al*, 2016.

[42] Pogledati rad Vie *et al,* 2015. Dodatno, o medicinskim bazama podataka u američkoj vojsci pogledati na stranici američkog Centra za podatke o ljudstvu u odbrani (eng. Defence Manpower Data Center).

[43] Široka lista biomedicinskih arhiva može se naći kod Toga & Dinov, 2015, pp. 4-5.

[44] Tekst zakona dostupan na http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm

[45] Sadržaj zakona pogledati na
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id

Istovetnu pravnu regulativu je usvojio i nemački parlament potvrdivši amandman iz 2016. godine u zakonu o nadležnostima obaveštajne službe (nem. Bundesnationaldienst-Gesetz); amandman saveznog zakona o zaštiti podataka (nem. Bundesdatenschutzgesetz) koji traži širu upotrebu video nadzora na javnim mestima bio je planiran[46] za usvajanje u 2017. godini. Izmenama se omogućava veća kontrola telekomunikacionog saobraćaja građana u zemlji i inostranstvu.

Amandmanima u periodu od 2006. do 2008. godine, američki zakon o nadgledanju inostranih državljana (eng. Foreign Intelligence Surveillance Act[47]) stvara zakonsku mogućnost državnim službama bezbednosti da preuzimaju podatke o telekomunikacionoj aktivnosti inostranih građana na i van teritorije SAD-a. Posebnu stavku na ovoj liniji gledanja predstavlja projekat Prizma (eng. PRISM) koje su američke vlasti pokrenule radi prikupljanja obaveštajnih podataka o građanima i naročito inostranim građanima. Kompanije poput Facebook-a, Google-a, Twitter-a, uz telekomunikacione kompanije davaoce usluga, su dužne da predaju podatke obaveštajnim službama.

Među glavnim dobavljačima (proizvođači softvera) u navedenom projektu su bile izraelske kompanije *Narus* i *Verint*. Izrael spada u prvih pet država na svetu prema broju kompanija u sektoru obaveštajnog rada.[48] Kompanije iz ove države u 2014. imaju 10% svetskog učešća u izvozu usluga sajber-obaveštavanja.[49] Istovremeno obaveštajno-bezbednosne agencije u Izraelu imaju dozvolu za preuzimanjem podataka o građanima bez saglasnosti sudskih organa.[50] Prema zakonu o biometrijskim metodama i čuvanju podataka iz 2009. godine Ministarstvo unutrašnjih poslova poseduje bazu podataka svakog građanina Izraela sa biometrijskim podacima (slika lica, otisci prstiju, krvna grupa) koji se skladište sa ostalim podacima (npr. poreski broj, zdravstveni karton, bankarski račun).[51] Služba unutrašnje bezbednosti – Šin Bet (eng. Shin Bet) bez sudske dozvole može da preuzme celokupan protok podataka u mobilnoj telefoniji bilo kog građanina.[52]

Centar bezbednosti informacija, podružnica ruske Savezne bezbednosne službe, je juna 2010. raspisao tender za nabavku softvera za analitičku pretragu medija i interneta[53]. Softverski paket „Semantička arhiva“ služi pretrazi medijskih sadržaja i generisanju zaključaka; poseban aspekt softvera je analiziranje mišljenja u blogovima i forumima na internetu. Izmenama ruskog saveznog zakona o kriminalnim postupcima br. 375-F3 usvojenim jula 2016. stavlja se obaveza pred operatore mobilne telefonije i internet usluga da snimaju, skladište i čuvaju potpun mobilni/internet saobraćaj svojih pretplatnika to-

[46] Najava amandmana dostupna na zvaničnoj stranici Vlade SR Nemačke https://www.bundesregierung.de/Content/DE/Artikel/2016/12/2016-12-21-bessere-videoueberwachung.html

[47] Prvobitni zakon videti na zvaničnoj internet stranici Vlade SAD-a. Amandmani su: 2006; 2007 i 2008.

[48] Podaci preuzeti iz izveštaja organizacije Privacy International 2016, p. 18. Izveštaj je dostupan na https://www.privacyinternational.org/node/911

[49] Financial Times, https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c

[50] Uredbom o procedurama kriminalnih aktivnosti (eng. Criminal Procedure Act) usvojenom 2007. omogućen je nesmetan pristup podacima internet i mobilne telefonije svakog građanina. Više detalja videti u tekstu J. Klinger (10.06.2013) dostupnom na https://2jk.org/english/?p=350

[51] Sиže teksta zakona dostupan na https://www.loc.gov/law/foreign-news/article/israel-law-on-biometric-methods-and-data-preservation/

[52] Pročitati kod Stevens (2011, p. 7).

[53] Podaci dostupni na http://agentura.ru/english/projects/Project_ID/blogs/

kom tri godine i učine ga dostupnim ovlašćenim državnim organima po njihovom zahtevu, *inter alia.*[54]

Zakon o sajber-bezbednosti (eng. *Cybersecurity Law*), prvi takve vrste u NR Kini donet je krajem 2016. godine a koji je stupio na snagu 1. juna 2017. godine, produžava vreme skladištenja internet i telefonskog saobraćaja kod operatera na šest meseci.[55] Pri tom, operateri su dužni[56] da učine sadržaj svojih baza podataka o korisnicima dostupnim odgovarajućim državnim organima (npr. Kancelarija centralne vodeće grupe za poslove sajber-prostora[57]) prema potrebi.

Japanske vlasti su 2003. usvojile Zakon o zaštiti ličnih informacija. Članom 23. tog zakona stav jedan, dozvoljen je pristup podacima operatera od strane državnih organa uz sudsko ovlašćenje.[58] Postoji pet navedenih izuzetaka pod kojima je dozvoljeno operateru da prosledi podatke trećoj strani.[59]

Nameće se zaključak o prisutnoj potrebi državnih organa za dostupnošću podataka svojih građana radi kontrole, analize i praćenja aktivnosti pojedinaca ili grupa, iz ekonomskih, bezbednosnih ili čisto političkih razloga. Time se argumentuje neophodnost postojanja analitičkog odeljenja *Big Data* u vojno-bezbednosnim strukturama zemlje čijim se radom adekvatno manipuliše podacima i stvaraju bitne informacije.

Uloga analitike velikih baza podataka pri sajber pretnjama

Digitalni format, obim, veličina i frekventnost podataka predstavljaju izvor informacija ali i izazov njihove obrade za vojno-obaveštajne službe. Primeri su podaci iz medicinskih kartona (krvna grupa, visina, težina, boja očiju); turistička putovanja (učestalost, dužina, destinacije, način putovanja); finansijski podaci (broj računa, poreski broj, sredstva na računu, promet plaćanja); popis stanovništva; komercijalni podaci (detalji operacija pravnih i fizičkih lica na tržištu); podaci o plaćenim ili pretplatničkim računima; promet na internetu i fiksnom-mobilnom saobraćaju (razgovori, korespodencija, slike, video zapisi); državni podaci o pojedincima.[60] „Veličina baza podataka varira u opsegu od stotina do miliona unosa koji se mogu međusobno povezati preko određene varijable (npr. telefonski broj) i time brzo steći uvid u sve podatke vezane za konkretnu osobu koja je predmet analize".[61] Sprečavanje kriminalnih dela, terorističkih ili subverzivnih postupaka podrazumeva praćenje mnoštva pojedinaca radi pronalaženja nekolicine odgovornih. Godišnji troškovi sajber-kriminala poput krađe informacijskih dobara, onemogućavanja usluga *inter alia*, su procenjeni na 118 milijardi $ godišnje.[62] *Big Data*

[54] Pročitati više u izveštaju ICNL (2016, pp.6-7) http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf

[55] Kompletan tekst zakona dostupan na http://www.chinalawtranslate.com/cybersecuritydraft/?lang=en#_Toc424040670

[56] Zakonom se kategoriše i definiše internet i telefonski saobraćaj kao i načini pružanja usluga operatera. Neke od posebnih osobenosti zakona mogu se naći u tekstu kod Ruan (2016); Kanner & Ella (2017).

[57] Zvanična internet stranica kancelarije (kineska verzija) www.cac.gov.cn

[58] Tekst zakona dostupan na http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

[59] Pogledati više kod Raul (2014, pp. 162-163).

[60] Izveštaj Privacy International (2016), https://privacyinternational.org/node/853

[61] Pogledati stav 156. u publikaciji o Obaveštajno-bezbednosnom delovanju (eng. *Intelligence and Security*), dostavljenoj britaskom Donjem domu 12. marta 2015.

[62] http://assets.teradata.com/resources/ebooks/102914-CyberSecurity-eBook/FLASH/index.html

analitika omogućava učinkovitije delovanje vojno-obaveštajnih agencija time što se smanjuje vreme pretrage voluminoznih podataka, povećava brzinu procesuiranja prikupljenih nestrukturiranih podataka, čime se uočavaju skriveni šabloni i spoznaju anomalije ili slične informacije koje mogu služiti boljem i bržem odlučivanju pri kriminalnim ili subverzivnim aktivnostima. Prednost je omogućena time što analitičari na početku analize ne moraju znati šta je cilj analize na samom početku, već se do toga dolazi tokom postupka analize.[63] U svom radu Horsman & Conniss (2015, p. 91) ukazuju na stepen anonimnosti koji uhodilac stiče korišćenjem pripejd mobilnih kartica i aplikacija na telefonu; dalje se ukazuje na značaj digitalnih forenzičara koji mogu da uđu u trag sajber progoniteljima putem korišćenih aplikacija. Od osam oglašenih radnih mesta za visokokvalifikovanu radnu snagu nemačke Obaveštajne službe (nem. *Bundesnachrichtendienst*), oko 67% čine radna mesta za informatičare i specijaliste sajber-infrastrukture.[64] U trenutku pisanja ovog rada u medijima je naveden slučaj neovlašćenog sajber uzurpiranja informacionih sistema u engleskim bolnicama i bankama.[65] Pravovremenost javljanja neovlašćenog pristupa u privatnoj mreži korisnika putem praćenja komunikacionih kanala kompjuterskih jedinica u jedinici vremena jeste prednost *Big Data* analitike.[66] Kriminalni delikti poput izbegavanja poreskih plaćanja, korišćenja lažnih bankarskih računa, malverzacija u penzijsko-invalidskom osiguranju se kontrolišu primenom analitike voluminoznih podataka. Troškovi nastali prevarama u američkom zdravstvenom osiguranju iznose godišnje 60 milijardi $.[67] Neovlašćeni pristupi internet sadržajima i bazama podataka ministarstava i državnih agencija su učestali postupci kojima se narušava bezbednost zemlje.[68] Troškovi reparacije krađe tuđe svojine (uključujući intelektualnu svojinu poput privatnih podataka građana) prouzrokovani sajber kriminalom se u velikim organizacijama u Engleskoj procenjuju na 275-375 hiljada £.[69] Natpisi i sadržaji na društvenim mrežama, najave u medijima država uzimaju se kao vrednosne promenljive na osnovu kojih se vrše predviđanja verovatnoća dešavanja u budućnosti poput protesta, pokreta, sklapanja ugovora, vojnih intervencija.[70] U okvirno 60 lokalnih policijskih ispostava u SAD-a se koristi softverski paket za predviđanje verovatnoće i lokacije budućih zločina na osnovu podataka iz prošlosti. Društveni mediji se karakterišu kao dragoceni izvor podataka za praćenje mogućih terorističkih grupacija.[71] Propagandno širenje

[63] SAS (2017) https://www.sas.com/en_us/insights/articles/risk-fraud/how-intelligence-agencies-reap-rewards-big-data.html

[64] http://www.bnd.bund.de/DE/Karriere/Stellenanzeigen/Hoeherer_Dienst/gentable_hd.html

[65] Onemogućavanje prethodno zakazanih operacija pacijenata, lažno alarmiranje ambulanti, uklanjanje medicinskih podataka pacijenata su prijavljeni u oko 116 engleskih i škotskih bolnica. Saopštenje je izdala premijer Velike Britanije Tereza Mej kao i engleski centar za nacionalnu sajber bezbednost. https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

[66] Harris, S. (2015). The Catch-22 In Cyber Defence: More Isn`t Always Better, Teradata: USA. Pristupljeno 14.05.2017. na http://assets.teradata.com/resourceCenter/downloads/Articles/EB8891.pdf?processed=1

[67] Informacije dostupne u radu Kambatla *et al.* (2014, r. 2570).

[68] Australijski Direktorat odbrambenih signala (eng. *Defence Signals Directorate*) je u 2010. godini zabeležio prosečno 700 napada na baze podataka vojnih agencija (AAP, 2010). U periodu od 2000. do 2010. se beleži tendencija neovlašćenog ulaska u poverljive sadržaje američkog Ministarstva odbrane Report to Congress (2010, r. 237).

[69] Uporedni pregled troškova videti u radu Low (2017, p. 19).

[70] Kao primer se može uzeti projekat MERKUR (eng. Mercury) finansiran od strane američke nacionalne obaveštajne službe sa ciljem predviđanja socijalnih nemira, epidemija bolesti, vojnih konfrontacija. Informacije dostupne na https://www.iarpa.gov/index.php/research-programs/mercury

[71] Dodatne informacije dostupne u novinskom članku Strohm (13. oktobar 2016).

džihadističkih ideja, regrutacija radikalnih muslimana, organizacija, povezivanje, prikupljanje finansijskih sredstava se obavlja preko sajber-prostora (internet).[72] Analitičko odeljenje vojno-obaveštajne službe mora posedovati kapacitet obrade takvih sadržaja u kratkom vremenskom intervalu. Oslanjanje na softver i algoritme u analitičkom radu stvara *automatizaciju* u obaveštajnom radu; pomeranje fokusa na pretpostavke o budućim ishodima stavlja *pretpostavljanje* u prvi plan analitičkog odlučivanja; tendencija *prilagođavanja* se odnosi na promenu metoda obaveštajnog rada shodno oblastima u kojima se definiše predmet analize.[73]

Zaključak

Primena savremenih tehnologija ima značajnu ulogu u rezultatima vojnih operacija i kontra-obaveštajnom radu. Stvaranjem analitičkih odeljenja pri vojnim jedinicama i obaveštajnim službama, koja se u svom radu oslanjaju na analitičke instrumente velikih baza podataka zapravo se podstiče rast učinkovitosti u radu i rezultatima. Primeri izloženi u radu ukazuju na nedvosmislenu potrebu mnogih razvijenih zemalja da u svojim vojno-bezbednosnim strukturama proces donošenja odluka u vojno-policijskim operacijama učine parcijalno zavisnim od stvorenih informacija. Ekstenzivnost dostupnih podataka uslovljena postojanjem tehničkih uređaja čija se očitavanja povezuju internetom predstavlja izazov ali i resurs. Autori ukazuju na bitnost pravilnog i potpunog tumačenja takvih podataka u ograničenom vremenskom periodu vojnih operacija i/ili obaveštajnog rada. Značajna finansijska ulaganja drugih zemalja u vojne resurse kojima bi se stekla sposobnost akumulacije podataka i njihovog čitanja primenom analitike *Big Data* jeste savremeni trend.

Na drugoj strani treba istaći etički problem dostupnosti i prikupljanja velikih baza podataka kojima se najčešće narušava pravo na privatnost pojedinca (slučajevi obaveštajnih službi) ili suverenitet zemlje (slučaj sajber špijunaže). Drugo, postoji problem tehničko-tehnološke zavisnosti strane koja otkupljuje tehnologiju. Time se podređena situacija vojske zemlje uvoznice čini ranjivijom usled nemogućnosti obrane od neovlašćenog protoka informacija ka zemlji izvoznici tehnologije. Dalje, ne treba izuzeti ekonomski aspekt i visoku cenu ulaganja u takvu tehnologiju koja nije dostupna *ad hoc* manje razvijenim zemljama. Treba primetiti i nedostupnost detaljnih podataka u stranim medijima koji se tiču tehničkih karakteristika i detalja domena primene analitike voluminoznih podataka.

Značaj ovog članka se ogleda u usmeravanju pažnje donosilaca odluka ka osavremenjivanju metoda obaveštajnog rada u vojnim i civilnim službama. Kvalitativnom analizom zasnovanom na uporednom pregledu vojnih trendova u izabranom uzorku stranih zemalja ispunjava se istraživački cilj: normativno približavanje savremenih tokova u vojno-obaveštajnom sektoru uslovima u našoj zemlji. Drugim rečima posmatranje i uočavanje progresivnih ideja koje se mogu adaptirati našim vojnim uslovima. Ideja za koju se autori zalažu se ogleda u primeni velikih baza podataka u našim bezbednosnim strukturama putem razvijanja infrastrukture, tehnologije i kadrova radi relativnog „pariranja“ vodećim zemljama. Autori posebno ističu primer Izraela i njegovog vojnog modela upotrebe analitike voluminoznih poda-

[72] O pregledu pretnji u sajber prostoru pročitati rad Choo (2011).

[73] Vrlo zanimljiv osvrt na temu upotrebe velikih baza podataka u obaveštajnom radu je u svom naučnom članku ponudio Lyon (2014).

taka. Budući istraživački pravac analize bi imao za cilj stvaranje domaćeg prototipa *Big Data* analitike u okviru Vojske Srbije ili njenih obaveštajnih agencija, merenje rezultata, poređenje sa drugim zemljama, prospekt izvoza osvojene tehnologije namenske industrije.

Reference

[1] Song., X., Wu, Y., Ma, Y., Cui, Y., Gong, G. (2015). Military Simulation Big Data: Background, State of the Art, and Challenges. *Mathematical Problems in Engineering* 2015 Article ID 298356. Pristupljeno 09.04.2017. na https://www.hindawi.com/journals/mpe/2015/298356/

[2] Couch, N., Robins, B. (2013). Big Data For Defence and Security. Royal United Services Institute. London, UK. Pristupljeno 05.04.2017. na https://uk.emc.com/campaign/bigdata/rusi/big-data-for-defence-and-security-report-final.pdf

[3] McAfee, A., Brynjolfsson, E. (2012). Big Data: The Management Revolution. *Harvard Business Review* , pp. 60-68. Pristupljeno 09.04.2017. na http://www.rosebt.com/uploads/8/1/8/1/8181762/big_data_the_management_revolution.pdf

[4] Rayport, J. (2012). Use Big Data To Predict Your Customers` Behaviours. *Harvard Business Review.* Pristupljeno 10.04.2017. na https://hbr.org/2012/09/use-big-data-to-predict-your-c

[5] Kosinski, M., Stillwell, D., Graepel, T. (2013). Private Traits And Attributes Are Predictable From Digital Records Of Human Behavior. Proceedings of the National Academy of Sciences of the United States of America. April 9, 2013, 110 (15), p. 5802-5805. Pristupljeno 10.04.2017. na http://www.pnas.org/content/110/15/5802.full

[6] Labrinidis, A., Jagadish, H. V. (2012). Challenges And Opportunities With Big Data. *Proceedings of the VLDB Endowment* 5 (12), pp. 2032-2033. Pristupljeno 11.04.2017. na http://dl.acm.org/citation.cfm?doid=2367502.2367572

[7] Gandomi, A., Haider, M. (2015). Beyond the Hype: Big Data Concepts, Methods, And Analytics. *International Journal of Information Management,* 35 (), pp. 137-144. Pristupljeno 11.04.2017. na http://ac.els-cdn.com/S0268401214001066/1-s2.0-S0268401214001066-main.pdf?_tid=9f8922c8-1fb1-11e7-a894-00000aab0f02&acdnat=1492023520_8b08508a4d39fd537cac350a3eca4b31

[8] Barbier, G., Liu, H. (2011). Data Mining In Social Media. *In* C. C. Aggrawal (Ed.), Social Network Data Analytics (pp. 327-352). United States: Springer. Pristupljeno 11.04.2017. na https://pdfs.semanticscholar.org/8a60/b082aa758c317e9677beed7e7776acde5e4c.pdf

[9] Gundencha, P., Liu, H. (2012). Mining Social Media: A Brief Introduction. *Tutorials In Operation Research*, 1 (4), pp. 1-17. Pristupljeno 11.04.2017. na http://pubsonline.informs.org/doi/pdf/10.1287/educ.1120.0105

[10] Gu, J., Zhang, L. (2014). Data, DIKW, Big Data and Data Science. *Procedia Computer Science* 31, pp. 814-821. Pristupljeno 11.04.2017. na http://ac.els-cdn.com/S1877050914005092/1-s2.0-S1877050914005092-main.pdf?_tid=8f3ab6f6-1fb2-11e7-af15-00000aab0f27&acdnat=1492023922_a67536b31ef42db4e8bd4b9593d0e5c6

[11] IDC (2016). Double-Digit Growth Forecast For the Worldwide Big Data and Business Analytics Market Through 2020. IDC Research, Inc. Pristupljeno 12.04.2017. na http://www.idc.com/getdoc.jsp?containerId=prUS41826116

[12] IDC. (2017). Big Data And Business Analytics Revenues Forecast. Worldwide Semiannual Big Data and analytics spending guide, International Data Corporation Research Inc.: Massachusetts USA. Pristupljeno 12.04.2017. na http://www.idc.com/getdoc.jsp?containerId=prUS42371417

[13] Columbus, L. (2016). Roundup Of Analytics, Big Data & BI Forecasts And Market Estimates, 2016. Forbes:USA. Pristupljeno 12.04.2017. na https://www.forbes.com/sites/louiscolumbus/2016/08/20/roundup-of-analytics-big-data-bi-forecasts-and-market-estimates-2016/#292fddb16f21

[14] Vesset, D., Schubmehl, D., Olofson, C., Gopal, C., Bond, S. (2016). Worldwide Business Analytics Software Market Shares, 2015. International Data Corporation. Pristupljeno 13.04.2017. na https://www.sas.com/content/dam/SAS/en_us/doc/analystreport/idc-business-analytics-software-market-shares-108014.pdf

[15] IIA. (2016). Advanced Analytics & Big Data Adoption Report. Dell Digital Business Services: International Institute for Analytics. Pristupljeno 13.04. 2017. na http://iianalytics.com/analytics-resources/advanced-analytics-big-data-adoption-report-2016

[16] Turck, M. (2016). Is Big Data Still a Thing? (The 2016 Big Data Landscape), World Press. Pristupljeno 12.04.2017. na http://mattturck.com/big-data-landscape/#more-917

[17] Department of Defence. (2016). Defense Budget Overview, Office of the under-secretary of defence: USA. Pristuljeno 14.04.2017. na http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_Budget_Request_Overview_Book.pdf

[18] Jones, S., (2016) . Ministry Of Defence Steps Up cyber security operations, Financial Times Ltd: UK. Pristupljeno 14.04.2017. na https://www.ft.com/content/73fbae2c-f81c-11e5-96db-fc683b5e52db

[19] Young , C. (2012). The Military`s New Challenge: Knowing What They Know. *Harvard Business Review*. Pristupljeno 14.04.2017. na https://hbr.org/2012/09/the-militarys-new-challenge-knowing

[20] Deltek. (2015). Top 20 Unrestricted Federal Business Opportunities For Fiscal Year 2016. Deltek Federal Information Solutions: Virginia, USA.Pristupljeno 13.04.2017. na https://www.deltek.com/en/products/business-development/govwin/modules/federal-market-intelligence

[21] Defence Technical Information Center. (2017). Budget Information. Department of Defence, USA. Pristupljeno 13.04.2017. na http://www.dtic.mil/dodinvestment/#/advancedSearch

[22] Kirk, A. (Oktobar 27. 2015). What Are the Biggest Defence Budgets In the World? The Telegraph: UK. Pristupljeno 13.04.2017. na http://www.telegraph.co.uk/news/uknews/defence/11936179/What-are-the-biggest-defence-budgets-in-the-world.html

[23] Guzelyte, S. (2016). National Defence Data 2013-2014 and 2015. (est.). European Defence Agency: Ixelles, Belgium. Pristupljeno 13.04.2017. na https://www.eda.europa.eu/info-hub/defence-data-portal

[24] EDA. (2016). Annual Report 2016. European Defence Agency: Brussels, Belgium. Pristupljeno 13.04.2017. na https://www.eda.europa.eu/info-hub/publications

[25] Lockheed Martin Corporation. (2017). 2016 Annual Report. Lockheed Martin Corporation, Maryland: USA. Pristupljeno 22.04.2017. na http://www.lockheedmartin.com/us/news/annual-reports.html?_ga=1.131306184.697988966.1492849339

[26] Starr, S. (2003). C4ISR Assessment: Past, Present, and Future. 8th International Command and Control Research & Technology Symposium, Washington: USA. Pristupljeno 22.04.2017. na http://dodccrp.org/events/8th_ICCRTS/pdf/059.pdf

[27] Kulshrestha, S. (2016). Big Data In Military Information and Intelligence. IndraStra Global. Pristupljeno 22.04.2017. na https://figshare.com/articles/Big_Data_in_Military_Information_Intelligence/2066640

[28] Fahey, S. (2012). Big Data And Analytics For National Security. Stanford University. Pristupljeno 05.04.2017. na http://web.stanford.edu/group/mmds/slides2012/s-fahey.pdf

[29] Yang, S., Yang, M., Wang, S., Huang, K. (2016). Adaptive Immune Genetic Algorithm For Weapon System Portfolio Optimization In Military Big Data Environment. *Cluster Computing,* 19 (3), pp. 1359-1372. Pristupljeno 23.04.2017. na https://link.springer.com/article/10.1007/s10586-016-0596-3

[30] Xu, Z., Liu, Y., Mei, L., Hu, C., Chen, L. (2015). Semantic Based Representing And Organizing Surveillance Big Data Using Video Structural Description Technology. *The Journal of Systems and Software* 102, pp. 217-225. Pristupljeno 23.04.2017. na http://www.sciencedirect.com/science/article/pii/S0164121214001551

[31] Kim, Y.H., Kang, H.G., Lee, J.K. (2017). Can Big Data Forecast North Korean Military Aggression? *Defence and Peace Economics,* online 23. Jan 2017, pp. 1-18. Pristupljeno 27.04.2017. na http://dx.doi.org/10.1080/10242694.2016.1270736

[32] MacDonald, B., Ferguson, C. (2015). Chinese Strategic Missile Defence: Will It Happen, and What Would It Mean?. Arms Control Association: Washington, USA. Pristupljeno 27.04.2017. na https://www.armscontrol.org/ACT/2015_11/Features/Chinese-Strategic-Missile-Defense-Will-It-Happen-and-What-Would-It-Mean

[33] Jahedi, S., Wenger, J., Yeung, D. (2016). Using Big Data To Identify the Concerns Of Potential Army Recruits. RAND Arroyo Centre Personnel, Training and Health Program: RAND Corporation, USA. Pristupljeno 24.04.2017. na https://www.rand.org/pubs/research_reports/RR1197.html

[34] Vie, L., Scheier, M., Lester, P., Ho, T., Labarthe, D., Seliqman, M. (2015). The U.S. Army Person-Event Data Environment: A Military-Civilian Big Data Enterprise. *Big Data,* 3(2), pp. 67-79. Pristupljeno 22.04.2017. na https://www.ncbi.nlm.nih.gov/pubmed/27447431

[35] Toga, A., Dinov, I. (2015). Sharing Big Biomedical Data. *Journal of Big Data,* 2 (7), pp. 1-12. Pristupljeno 23.04.2017. na https://journalofbigdata.springeropen.com/articles/10.1186/s40537-015-0016-1

[36] Stevens, A. (2011). Surveillance Policies, Practices and Technologies In Israel And the Occupied Palestinian Territories: Assessing the Security State. *The New Transparency,* Working Paper IV, Social Sciences and Humanities Research Council of Canada. Pristupljeno 27.04.2017. na www.sscqueens.org/sites/default/.../2011-11-Stevens-WPIV.pdf

[37] Nonaka, T. (2014). Japan. In Raul, A. (Eds). *The Privacy, Data Protection and Cybersecurity Law Review*. Law Business Research Ltd, London: UK. Pristupljeno 13.05.2017. na https://www.sidley.com/en/insights/publications/2014/11/the-privacy-data-protection-and-cybersecurity-law-review

[38] Committee of Parliament. (2015). Privacy And Security: A Modern And Transparent Legal Framework. House of Commons, London: UK. Pristupljeno 14.05.2017. na https://sites.google.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attredirects=1

[39] Horsman, G., Conniss, L. (2015). An Investigation Of Anonymous And Spoof SMS Resources Used For the Purposes of Cyberstalking. *Digital Investigation* 13, pp. 80-93. Pristupljeno 10.05.2017. na https://doi.org/10.1016/j.diin.2015.04.001

[40] Kambatla, K., Kollias, G., Kumar, V., Grama, A. (2014). Trends In Big Data Analytics. *Journal of Parallel and Distributed Computing* 74 (7), pp. 2561-2573. Pristupljeno 15.05.2017. na http://www.sciencedirect.com/science/article/pii/S0743731514000057

[41] Choo, K. (2011). The Cyber Threat Landscape: Challenges And Future Research Direction. *Computers and Security* 30, pp. 719-731. Pristupljeno 15.05.2017. na http://www.sciencedirect.com/science/article/pii/S0167404811001040

[42] Low, P. (2017). Insuring Against Cyber-Attacks. *Computer Freud and Security* 4, pp. 18-20. Pristupljeno 16.05.2017. na http://www.sciencedirect.com/science/article/pii/S1361372317300349

[43] Strohm, C. (2016). Predicitng Terrorism From Big Data Challenges U.S. Intelligence, Bloomberg: USA. Pristupljeno 15.05.2017. na https://www.bloomberg.com/news/articles/2016-10-13/predicting-terrorism-from-big-data-challenges-u-s-intelligence

[44] Lyon, D. (2014). Surveillance, Snowden, And Big Data: Capacities, Consequences, Critique. *Big Data and Society* 1(2), pp. 1-13. Pristupljeno 16.05.2017. na http://journals.sagepub.com/doi/pdf/10.1177/2053951714541861