DIGITALNA TRANSFORMACIJA SIGURNOSTI I ALGORITAMSKA DEMOKRATIJA

Article · April 2021

CITATIONS
2

READS
19

1 author:

Emir Vajzovic
University of Sarajevo
17 PUBLICATIONS **104** CITATIONS

SEE PROFILE

Vajzović, Emir (2020) Digitalna transformacija sigurnosti i algoritamska demokratija. Sarajevo Social Science Review 9(2), 2020.

DIGITALNA TRANSFORMACIJA SIGURNOSTI I ALGORITAMSKA DEMOKRATIJA

EMIR VAJZOVIĆ[1]

Fakultet političkih nauka Univerzitet u Sarajevu

Bosna i Hercegovina

SAŽETAK

Rad se fokusira na aspekte kritičko-sigurnosnih studija prateći kontekst informacijskog nereda u složenom komunikacijskom, medijskom, obrazovnom, političkom okruženju kao i mogućnosti apomedijacije u kontekstu sigurnosnih izazova. Namjera je naglasiti kako se tradicionalni sistemski filteri kontrole i verifikacije informacija (*gatekeeperi*) destabilizirani "digitalnim stanjem" (referencijalnost, komonalnost, algoritmičnost) koje teret poimanja političke, pa tako i sigurnosne kulture, pomjera ka razumijevanju postdemokratskog društva. Algoritamska amplifikacija novih društvenih, demokratskih i sigurnosnih odnosa stvara novu dimenziju društveno-političko-tehnoloških odnosa, koje u ovom radu pokušavamo obuhvatit sintagmom algoritamska demokratija. Savremeni razvoj može, u sigurnosnom smislu, biti velika opasnost, ali u isto vrijeme i velika šansa za čovječanstvo i čovjeka kao pojedinca. Ključno je građansko osnaživanje obrazovanjem za digitalno doba, tj. preciznije: podizanje nivoa medijske i informacijske pismenosti kako bi se uloga *gatekeepera* u suvremenom informacijsko-komunikacijskom okruženju, vratila u ruke ljudi, a ne mašina.

Ključne riječi: Digitalna transformacija sigurnosti, algoritamska demokratija, medijska i informacijska pismenost.

ABSTRACT

The paper is focusing on aspects of critical security studies following the context of information disorder in a complex communication, media, educational, political environment as well as the possibilities of apomediation in the context of security challenges. The intention is to emphasize how traditional information gatekeepers destabilized by the "digital condition" (referentiality, communality, algorithmicity) which shifts the burden of understanding political, and thus security culture, towards understanding post-democratic society. Algorithmic amplification of new social, democratic and security relations creates a new dimension of socio-political-technological relations, which in this paper we try to understand trough algorithmic democracy. Modern development can, in terms of security, be a great threat, but at the same time a great chance for humanity and man as an individual. The key is civic empowerment through education for the digital age, or more precisely: raising the level of media and information literacy in order to regain the role of gatekeepers in the modern information and communication environment to the hands of people, not machines.

Key words: Digital security transformation, algorithmic democracy, media and information literacy.

[1] Fakultet političkih nauka, Univerzitet u Sarajevu, Bosna i Hercegovina, emir.vajzovic@fpn.unsa.ba; Skenderija, 72, 71000 Sarajevo

"We shall squeeze you empty, and then we shall fill you with ourselves.

—George Orwell, 1984"

1. Uvod: Kritičke sigurnosne studije, informacije i građani

Ovaj bi se rad, u klasičnom naučnom pogledu, mogao smatrati multi/inter/kros-disciplinarnim. Ipak, pristup će biti antidisciplinarni[2], s obzirom da kritička teorija sigurnosti treba stati protiv kompartmentalizacije[3] znanja i podjela intelekta. (Neocleous, 2008; Roland, 1992) Savremene sigurnosne studije, u svjetlu antidisciplinarnosti ne stoje u opreci spram disciplina već, kako ističe J. Ito (2018), „istražuje ideje i istraživačke agende koje djeluju preko njih"[4], i prevazilaze nepotpun pristup problematici. Na to nas, na takav pristup, obavezuje kompleksnost digitalne transformacije društva, politike, pa shodno tome i sigurnosti, te direktne povezanosti sa medijskom i informacijskom pismenošću. Kako Krause i Williams (1997, str. 367) navode, „zadatak kritičkih sigurnosnih studija bio bi preoblikovati temelje sigurnosti i povezati ih s oblicima političke zajednice od kojih je odvojena raznim modernim praksama - od kojih je najmanje važna militarizacija." Osim osnovnih pitanja konflikta i sile, kroz ovaj novi kritički pristup vidjeli bismo sigurnost kao nadilaženje granica moderne države i rješavanje problema transnacionalne ranjivosti, te povezivanje sa *algoritamskom demokratijom*.

Ovu izazovnu temu razvijamo sa pozicije kritičkih studija sigurnosti i zasnivamo na hipotezi da je digitalna transformacija društva uzrokovala ne samo tehničko-tehnološke promjene u oblasti sigurnosti, već i promjene u sagledavanju demokratskog diskursa, kao i novih rizika i prijetnji. Polazimo sa gledišta da sa ovim transformacijama sve je značajnija uloga aktivnog građanina, kao elementa snaga sigurnosti (Beridan, 2008), jer uslijed apomedijacije u složenom medijskom, informacijskom, obrazovnom, političkom i sigurnosnom okruženju, tradicionalni sistemski filteri gube svoju pretpostavljenu ili očekivanu ulogu, te većinu tereta poimanja društveno-političke zbilje, pa i sigurnosne kulture, prepoznavanja prijetnji i rizika, preuzimaju na sebe sami građani (Vajzović 2019; 2020). Stoga, medijska i informacijska pismenost je u savremenom trenutku neophodan i poželjan elemenat sigurnosti pojedinca, organizacije, države i (post)demokratije. Postavlja se pitanje (istraživačko) u kojoj mjeri medijska i informacijska pismenost može biti (ključna) kompetencija viđena kao potrebna, ne samo na individualnom nivou, nego i za društvo i poimanje sfere sigurnosti.

---

[2] U članku „Cyberculture studies: An antidisciplinary approach", Mckenzie Wark ističke antidisciplinarnost kao političku agendu razumijevanja svijeta napuštanjem tradicionalnih akademskih disciplina. Wark (2006) ističe da kiberkultura nosi potencijal ne samo da bude nova disciplina već kraj disciplina koje održavaju oskudicu u znanju: "kiberkulturne studije mogu biti tačka iz koje oslobađanje znanja od oskudice započinje kao samosvjesni proces. Kiberkulturalne studije mogu biti kritička teorija, a ne hipokritička teorija, proizvodnje znanja iz sebe i za sebe (str. 72.). Vidi: Wark, M. (2006). Cyberculture studies: An antidisciplinary approach (version 3.0). In D. Silver & A. Massanari (Eds.), Critical cyberculture studies (pp. 68–78). New York: NYU Press

[3] Termin iz oblasti informacijske sigurnosti – proces i stanje ograničenog pristupa informacijama za osobe koje su izvan određenog klastera, odnosno grupe koja je upoznata samo sa određenim skupom informacija. „Vizantija je kompartmentalizirala znanje svog sistema (oružja, o.a.), tako da svako ko bi mogao pasti neprijatelju u ruke nema nego samo mali dio tajne." Roland,1992: 664. prevod autor.

[4] Antidisciplinarnost suočava sa izazovima izvan tradicionalno uspostavljenih granica. „Antidisciplinarni pristup može omogućiti zajednicama da nadiđu postojeće paradigme, a Internet pruža priliku da preustroji visoko obrazovanje i razvoj znanja i disciplina koji podržavaju takav pristup. (…) Opisujem ideju antidisciplinarnog rada između i izvan disciplina i napominjem da je to posebno važno jer je svijet postao složeniji i brži zahvaljujući Internetu." O antidisciplinarnom pristupu i programu vidjeti više u radu direktora MIT Media Lab-a, Joichi Ito. Ito, J. (2018). *Practice of Change* Doctoral dissertation. Keio University. Retrieved from https://www.practiceofchange.org/

Ovaj rad ima za cilj da teoretskim uklonom i naučnim metodama indukcije i dedukcije, analize i sinteze, odgovori na postavljene hipoteze, te u radu počinjemo od pregleda i opisa korelacije između ljudi i informacija, jer upravo ta međukompleksnost jest glavni određujući faktor „digitalnog stanja“ danas (Stalder, 2018). Značaj razvoja kompetencija medijske i informacijske pismenosti (MIP) kao šestog čula provlači se, praktično, kroz čitav rad ukazujući na značaj razumijevanja digitalne transformacije društva i sigurnosti, te njihove implikacije na demokratski diskurs. U konačnici, djelimično ćemo pokušati odgovoriti na pitanje uloge algoritama, umjetne inteligencije (AI) i tehno-kapitalizma u navedenim temama, te njihove povezanosti sa prijetnjama, rizicima i sigurnosti na državnom, korporativnom i individualnom nivou.

Budući da ćemo se u radu dosta susretati sa terminom *sigurnost*, za koji se u engleskom jeziku upotrebljavaju dva zasebna termina: *Safety* i *Security,* nužno se u tom pogledu nameće pitanje pojmovnog određenja u sigurnosnom terminosistemu, posebno u smislu kontekstualizacije sigurnosti sa digitalnom transformacijom društva, te činjenice da se u bosanskome jeziku data terminološka jedinica razumijeva uglavnom kao jedan termin sa svojim dvjema sinonimskim odrednicama (*sigurnost*, odnosno, *bezbjednost*), koje se u pravilu percipiraju kao „varijantski“ markirane vrijednosti, mada ima i tvrdnji da, kako navodi Dujević (2006, str. 139), „svestranija analiza ova dva termina nedvosmisleno pokazuje da su to različiti termini.“ Iz razloga takvoga terminološkog nesuglasja, u ovom će se radu koristiti termin *sigurnost* u njegovoj ukupnoj pojmovnoj kompleksnosti. Ipak, imajući u vidu engleski jezik kao *linga franca* današnjeg akademskog rada i interneta (i Mreže), poželjno je pojasniti termine i korespondirajuće odrednice. Terminom *Safety* se „iskazuje snaga i sposobnost djelovanja radi sprječavanja mogućeg razvoja nesigurne situacije odnosno sprječavanje uzroka mogućih sigurnosnih implikacija“, dok *Security* se više koristi u kontekstu nacionalne sigurnosti „s čim se označava ostvarenje, čuvanje i zaštita državnog nacionalnog interesa“ (Dujević, 2006, str. 139), tj. za potrebe razgraničavanja, možemo ih deskriptivno označiti i kao „aktivnu sigurnost“ (*Security*) naspram „preventivne sigurnosti“ (*Safety*). Tako se iz kontekstualnog značenja u rečenici: *„Security is therefore the process for ensuring our safety“* - može zaključiti da je aktivna sigurnost proces za osiguranje naše preventivne sigurnosti.

Unutar oblasti *informacijske sigurnosti*, glavni je cilj zaštititi povjerljivost, cjelovitost i dostupnost informacija, dok je sigurnost (*safety*) usmjerena na zaštitu života, zdravlja ili prirodnih utjecaja od bilo kakve štete koju sistemu mogu prouzročiti. Sigurnost (*security*) se usredotočuje na prijetnje koje dolaze izvan sistema, često uzrokovane zlonamjernim elementima, dok se sigurnost (*safety*) usredotočuje na nenamjerne događaje. Te razlike rezultiraju različitim osnovama za prioritiziranjem rješenja (Line, Tøndel, Nordland, Røstad, 2006).

U većini problematiziranja kritičkih teorija sigurnosnih studija autori se fokusiraju na državocentrični diskurs, međunarodnu i nacionalnu sigurnost, humanu sigurnost - u kontekstu međunarodnih odnosa, unutrašnje sigurnosti, policije, vojske, i rata kao klasičnog tako i mrežno-centričnog (Guha, 2011; Salter , Mutlu, 2013; Krause i Williams, 1997; Jacobs, Bayerl, Horton, Suojanen, 2021; Ramírez , Biziewski, 2020; Cavelty , Balzacq, 2017; Smajić, Seizović, Turčalo, 2017; Vajzović, Turčalo, Smajić, 2019; Turčalo, Smajić, Vajzović, 2019).

Ipak, postoje i drugi koji sagledavaju elemente nadzora, moći i „prizmu bioinformatičke fuzije čovjeka i tehnologije“ (Vajzović, 2020, str. 12), upravljanja populacijom, kroz inverziju čuvene Clausewitzove izreke da je „rat nastavak politike na druge načine“ (Clausewitz, Howard, 1993). Tako, naprimjer, Foucault (2002) i drugi autori nastoje istražiti u kojoj je mjeri politika, zapravo, „nastavak rata drugim sredstvima“ (Peoples, Vaughan-Williams, 2014, str. 161; Amoore 2009, str. 50; Foucault 2002, 2007), odnosno, u kojoj se mjeri sigurnosne prakse

uklapaju u napore za upravljanje kretanjem ljudi i nastojanjima da identifikuju, nadziru i obuzdavaju elemente stanovništva koji bi mogli predstavljati „sigurnosni rizik“ (Peoples, Vaughan-Williams, 2014, str. 161; vidjeti i: Collective, 2006).

U ovome radu fokus je na kritičkim sigurnosnim studijama u kontekstu informacija i ljudi, jer „usljed apomedijacije[5] u složenom medijskom, informacijskom, obrazovnom, političkom i sigurnosnom okruženju, tradicionalni sistemski filteri (*gatekeeperi[6]*) gube svoju pretpostavljenu ili očekivanu ulogu, te većinu tereta poimanja društveno-političke zbilje, pa i sigurnosne kulture, prepoznavanja prijetnji i rizika, preuzimaju na sebe sami građani“ (Vajzović, 2019, str. 532; vidjeti i: Moeller, 2020). Ta činjenica nužno ima i svoje refleksije na navike, vrijednosti, potrebe ljudi, ali i percepciju sebe i sigurnosti. Imamo novo stanje sa kapitalizmom nadziranja (Zuboff, 2019) i algoritamskom amplifikacijom novih društvenih, demokratskih i sigurnosnih odnosa, pri čemu “društveni ugovor više ne predstavlja odnos između građana i države, već korisnika i platformi društvenih medija”, i svakako zahtijeva promišljanje odnosa naroda, države i suvereniteta naspram tehnoloških kompanija (Lovink, 2018; Gunkel 2014; Hobbes 2009). Polazeći od toga, možemo reći da se stvara nova varijanta društveno-političko-tehnoloških odnosa u obliku algoritamske demokratije.

Na osnovu istraživanja i definisanja medijske demokratije (Vajzović, 2016; 2017, str. 273; Meyer i Hinchman, 2010), mogli bismo *algoritamsku demokratiju* definisati (i) kao oblik tvorbe političke volje i donošenja odluka, gdje jednu od ključnih pozicija u informativnom, obrazovnom, pa i političkom procesu preuzimaju algoritmi i umjetna inteligencija (umjesto prethodno: masovni mediji i njihova komunikacijska pravila), koji su tijesno povezani sa stepenom bioinformatičke fuzije čovjeka i tehnologije, medijske i informacijske pismenosti, neovisnosti regulatora (ne samo sektora komunikacija, nego prije svega prikupljanja i korištenja podataka, nadzora i kontrole nad algoritmima), općeg socio-ekonomskog stanja u državi i stepena digitalne transformacije društva.

Kao primjeri za analizu mogu poslužiti slučajevi Cambridge Analitika sa projektima Brexit i Trump (Podumljak, 2018; Amer, 2019; Graham-Harrison i Cadwalladr, 2018). Građani kao izvor podataka postaju predmetom tzv. *podacima vođene vladavine* (data-driven governance) budući da je njihovo upravljanje u rukama privatnih IKT[7] kompanija (Greenfield, 2013 u Hibert, 2020).

U nastavku teksta pokušat ćemo argumentacijom značaja medijske i informacijske pismenosti, zapravo preciznije kontekstualizirati digitalnu transformaciju sigurnosti. U Deklaraciji o značaju medijske i informacijske pismenosti u Bosni i Hercegovini (2019) daje se sveobuhvatna definicija:

[5] Apomedijacija (lat.) - akteri koji u kontekstu digitalnih medija zamjenjuju posrednike između korisnika i usluga (dakle informacija koje korisnici traže), što znači da sada stoje uz njih, osiguravajući dodatnu vrijednost izvana kao apomedijatori (Eysenbacha 2008). Drugim riječima kazano, „apomedijacija“ „tradicionalnu ulogu kao čuvara i posrednika odvodi prema ulogama vodiča, savjetnika i facilitatora (podržavatelja)“ (Kulenović 2018). Medijacija je važan koncept koji uključuje ekonomiju, pristup i moć. Tradicionalna vrsta posredovanja je posredovanje - to jest posredovanje između jedne i druge osobe ili između jedne osobe ili entiteta i resursa. Posrednici često blokiraju pristup ili ga na neki način ograničavaju. U nekim slučajevima posrednici postoje jer na djelu postoji model oskudice. Apomedizacija je neologizam stvoren uvođenjem latinskog izraza za "odvojeno, odvojeno, daleko od." (Anderson, 2008)

[6] Gatekeeper: eng. Vratar, čuvar vrata ili ključeva; osoba ili stvar koja kontrolira pristup nečemu. U ovom radu termin treba razumijevati kao tradicionalni sistemski elemenat koji nadgleda, filtrira i uređuje procese.

[7] IKT - informacijska i komunikacijska tehnologija, djelatnost i oprema koja čini tehničku osnovu za sustavno prikupljanje, pohranjivanje, obradbu, širenje i razmjenu informacija različita oblika, tj. znakova, teksta, zvuka i slike. (Hrvatska enciklopedija, mrežno izdanje)

> „Medijska i informacijska pismenost odnosi se na kognitivne, tehničke i socijalne vještine i sposobnosti građanki i građana da pristupaju, kritički ocjenjuju, koriste i doprinose informacijskim i medijskim sadržajima putem tradicionalnih i digitalnih informacijskih i medijskih platformi i tehnologija, uz razumijevanje kako te platforme i tehnologije djeluju, kako da prilikom njihovog korištenja upravljaju vlastitim pravima i poštuju prava drugih, kako da prepoznaju i izbjegnu štetne sadržaje i usluge, da svrsishodno koriste informacije, medijske sadržaje i platforme da bi zadovoljili svoje komunikacijske potrebe i interese kao pojedinci i kao pripadnici svojih zajednica, te da bi prakticirali aktivno i odgovorno učešće u tradicionalnoj i digitalnoj javnoj sferi i u demokratskim procesima.“

Ipak, ako mislimo da će razvoj vještina MIP-a, samo po sebi biti svrha i stoga (automatski) pozitivno doprinositi društvu, te moći raspoznati važnost informacija za demokratsko društvo, Kapitzke (2003) taj koncept smatra obrazovno ispraznim, beskorisnim i čak podmuklim, ukoliko kroz njega nije moguće eksplicitno raspoznati sociopolitičke i ideološke dimenzije informacija.

2. Od kolijevke pa do groba, najdraže je digitalno doba[8]

Homo sapiens[9] (*lat.;* umni čovjek), kao vječita misterija i područje introspektivne i retrospektivne analize i istraživanja na nivou ljudskih potreba, sistema vrijednosti, ali i pretpostavki za preživljavanje - od pamtivijeka se uzdao u podatke koje je prikupljao za potrebe donošenja informisanih i obrazovanih odluka na osnovu kojih je radio analizu sigurnosnih rizika i, sukladno tome, odgovarajućih mjera zaštite. Od početka, čovjek je obdaren sofisticiranim senzornim sistemom, za svoje potrebe, optimalnim omjerom osnovnih čula: vid, sluh, dodir, miris, okus. Na osnovu njih je isprva donosio sve odluke. To su dugo bili i jedini izvori podataka, koji su u datom kontekstu činili informaciju, pa informacije u korelaciji stvarale znanje, a znanje kroz vrijeme i iskustvo stvarale mudrost. (Rowley, 2007). Upravo je ta *diferencia specifica* umnosti i temelj logosa kod čovjeka, koji je „imanentan svemu postojećemu, on je kozmički princip koji uvodi poredak i umnost u svijet, kao što čovjekov um uređuje čovjekovo djelovanje“ (logos, Hrvatska enciklopedija, mrežno izdanje).

Na osnovu logosa, očekujemo razvoj kompetencija medijske i informacijske pismenosti, kao *šestog čula* potrebnog za sagledavanje sigurnosnih rizika, prostora političkog, te promišljeno, mudro, razvijanje mjera zaštite, posebno u kontekstu digitalne transformacije društva, sfere političkog i sigurnosti. Ipak, da bi nam logos omogućio shvatanje principa i oblika, potrebni su i temeljni ulazni podaci, ali i razumijevanje odnosa sa informacijama, znanjem i mudrosti. Prepoznatljiva DIKW[10] piramida/hijerarhija se može razumijevati na nivou kontekstualizacije, perspektive razumijevanja i vremenski (Brahmachary, 2019; Bosančić, 2017).

Vremenom je čovjek izgrađivao potrebu da svoje opažanje, informacije, znanje i mudrost podjeli sa drugima, direktno i preko sredstava za prenošenje informacija (počev od pećinskih crteža, glinenih ploča itd.), pa se tako razvijao jezik i pismo, kao i metode i materijali prenosa

---

[8] Remiks i kontekstualizacije tradicionalne pjesmice iz (SFRJ) obrazovnog sistema (ilirskog porijekla): *„Od kolijevke pa do groba, najljepše je đačko doba. Kad se kriju mnoge stvari, kad se pišu spomenari. Blago onom koji umije, đačko doba da razumije.“*

[9] Kako se kosmos ne vrti oko nas ljudi, potrebno je odrediti našu sistematiku tj. biološka klasifikaciju (znanstvena disciplina koja istražuje raznovrsnost organizama i njihove međusobne veze, i sastavni je dio taksonomije). Pri sistematiziranju je nužno uključiti što više parametara koji utječu na procese evolucije novih vrsta kako bi se utvrdila cjelovita filogeneza. Stoga, *Homo sapiens:* Sistematika: Carstvo:Animalia; Koljeno: Chordata; Razred: Mammalia; Red: Primates; Natporodica: Hominoidea; Porodica: Hominidae; Potporodica: Homininae; Tribus: Hominini; Rod: Homo; Vrsta: Homo sapiens (The Smithsonian Institution's Human Origins Program)

[10] Data-Information-Knolwdge-Wisdom

opažanja, doživljaja, događaja. Razvojem vizuelnog predstavljanja verbalne komunikacije stvaraju se i pouzdani(ji) oblici pohrane i prijenosa podataka. (Pra)čovjek počinje da komunicira sa drugima u prostoru i vremenu. Od tada se, suštinski, počinje razvijati i medijska i informacijska pismenost, tj. potreba za tim setom specifičnih kompetencija.

Osim toga, kako se vremenom razvijalo masovno komuniciranje (vidi: Nuhić 2000), koje je pratila akumulacija i čuvanje informacija, zatim primjena prakse, perspektive i alata upravljanja, pa prikupljanje, organizacija, čuvanje i širenje informacijskih izvora (Hibert, 2018; Stokić Simončić, 2016; Shera, Foskett, 1965), što je, naravno, snažno doprinosilo razvoju znanja - tako se uviđao i potencijal i potreba za statističkom i matematičkom obradom tih podataka i informacija (O'Neil, 2016). Podaci o podacima: meta-podaci počinju bivati vrlo vrijedan resurs, koji polako transformiše i stanje sigurnosti i stanje političkog u društvu.

Naporedo sa razvojem modernih država, i državnocentričnih sistema, javljaju se i sistemi provjera i propusnosti informacija (*gatekeeperi*): obrazovni sistemi, profesionalni mediji, biblioteke, arhivi, muzeji, regulatori sektora komunikacija, sigurnosni sistem(i) itd. U analognom dobu, njihova je funkcionalnost i efikasnost bila uglavnom na visini zadatka. Postojali su sistemski filteri koji su osiguravali da krajnji korisnik (građanin) ima visok stepen povjerenja u informacije koje dobija i na osnovu kojih funkcioniše.[11] S obzirom na to da je sfera informacija bila relativno uređena i posredovana, šesto čulo (MIP) biva manje izoštreno, dok je državocentrična sigurnost bila zadužena za zadovoljavajući nivo sigurnosti (realni i subjektivni) u fizičkom svijetu.

Digitalna transformacija sigurnosti može se posmatrati kao potreban odgovor na izraženu složenost savremenog sigurnosnog okruženja i pojave novih izvora nesigurnosti, prije svega u cyber prostoru i nevidljive ruke algoritama, upotpunjujući nedostatke državocentričnog okvira, ali i destabilizacije u sferi informacija, kao i distorzije[12] u sferi političkog i tržišnog. U tom kontekstu „sigurnosne prijetnje i izazovi izlaze iz okvira tradicionalnog poimanja međunarodno pravno definisanog i razumijevanog koncepta ratova (sukoba, konflikata), te ulazi u sferu hibridnih asimetričnih sigurnosnih izazova i ratova" (Vajzović, 2019, str. 532; vidjeti i: Schmitt, 2017).

Koristeći naše podatke generirane kroz digitalni trag, matematičari i statističari proučavaju potencijal naših želja, kretanja, potrošnje, te „predviđanje naše pouzdanosti i izračunavanje našeg potencijala kao učenika, radnika, ljubavnika, kriminalaca" (O'Neil, 2016:10), ali i glasača kojima još uvijek niko nije rekao da su u novom društveno-političko-tehnološkom uređenju algortamske demokratije. Hibert (2018) u vezi s tim navodi da „informacijsko-komunikacijske tehnologije nisu puki alati, već sile novog ekosistema koje utiču na našu percepciju sebe, interakcije i međusobne odnose, kao i predstavu stvarnosti (Floridi, 2015)"(…) Možemo reći da (…)„prožimajuća emergentnost *onlife* društvene entropije, proistekle iz "viška" (participacije) u novoj javnoj sferi, tako reaktualizira dijalektički naboj istraživanja odnosa moći u umreženom ekosistemu "crne kutije" (Pasquale 2015)" (Hibert, 2018, str 18).

Ovdje se naglašava potreba za medijskom i informacijskom pismenošću zasnovanom na principima cjeloživotnog učenja. Krovna je to „kompetencija koja se pretpostavlja u društvu koje je doživjelo digitalnu transformaciju i očekuje od građanina da je dovoljno informiran i

[11] Ovdje namjerno ne obrađujemo standardne kritike zloupotrebe vlasti i gatekeepera u nedemokratskim praksama i sistemima, jer su ovi već bili predmetom brojnih analiza i istraživanja, a sam rad bi dodatno odvelo u širinu.

[12] Prema Vajzović, 2019: Distorzija označava iskretanje, izvijanje, iskrivljenje; izopačenje, izobličenje; promjena izvornoga oblika tijekom manipulacije. U ovom kontekstu distorzija označava namjerno djelovanje na društveno-politički i sigurnosni sistem, sa ostvarivanjem političkog cilja.

obrazovan kako bi bio ravnopravan učesnik u demokratskom diskursu, te kao proaktivni samostalni subjekt, konstruktivno i odgovorno donosio odluke i doprinosio društvu znanja“ (Vajzović, 2020, str. 12). Bitno je shvatiti da „medijska i informacijska pismenost nije samoj sebi svrha, (…) već proces i pristup koji vraća „fabričke“ postavke filozofije demokratskog društva i poštivanja ljudskih prava i sloboda“ (Vajzović 2020, str. 12).

3. Sigurnost, ljudske potrebe i algoritmi

Vrsta sigurnosti ima mnogo, gotovo koliko i interesnih sfera svakog čovjeka: društvena sigurnost, politička, ekonomska, ekološka, zdravstvena, itd. Svaka od njih je podložna informacijskoj i medijskoj interpretaciji stvarnosti, i zavisno od stepena razvoja naših kompetencija medijske i informacijske pismenosti (MIP), sposobni smo donositi informisane, obrazovane i kritički promišljene odluke. Obdareni našim šestim čulom (u kontekstu kompetencije cjeloživotnog učenja) možemo se osjećati sigurno (*safe*) i donositi sigurnosno (*security*) promišljene odluke. Sigurnost je kompleksan i integralan pojam; za nju možemo reći da je „optimalana, poželjna i ohrabrujuća izvjesnost“. (Masleša, 2001); „sigurnost stoji naspram ugrožavanja, prijetnji i obrnuto“ (Beridan 2008, str. 25); ona je preduslov za razvoj i ostvarenje ljudskih prava i sloboda, ali i osnov razvoja društva u ekonomskom, kulturnom i političkom smislu. Stanje političke predvidivosti jedan je od značajnih segmenata poimanja sigurnosti, najvidljiviji kroz prizmu mirne promjene vlasti, vladavine prava, tj. pravnu državu kao pretpostavku ustavne demokratije, odnosno, kroz npr. „četvorodimenzionalan model demokratije, ukotvljen u četirima vrstama prava u koje mogu biti razvrstana sva osnovna prava: politička prava, građanska prava, prava na slobodu i socijalna prava“ (Ferrajoli, 2012). Društvenu sigurnost Masleša (2001, str. 19) definiše kao „stanje koje osigurava da se u poželjnim sigurnosnim okvirima i demokratskoj klimi sa vladavinom zakona i demokratskom kontrolom na svim nivoima vlasti, svim pojedincima obezbjedi i omogući praktikovanje rješavanje svojih egzistencionalnih i statusnih sadržaja u skoro svim oblastima života i rada, izgradnju međusubjektivnih odnosa s onu stranu nasilja poštivanjem svih postulata modernog demokratskog pravnog i civilnog društva.“

Mangold (1990) sigurnost definiše kao „stanje bez opasnosti i ugrožavanja, sigurnost podrazumijeva i osjećaj sigurnosti, ali i aktivnosti odnosno sistem za ostvarenje sigurnosti“. Tu subjektivnu dimenziju sigurnosti moguće je percipirati kao odsustvo osjećaja straha od ugrožavanja društvenih vrijednosti; dok se odsustvo prijetnji prema društvenim vrijednostima odnosi na objektivu dimenziju sigurnosti (Wolfers, 1962, str. 147-231). Možemo zaključiti da osiguranje i subjektivne i objektivne dimenzije sigurnosti (*Safety* i *Security)* podrazumijeva istodobno i zaštitu vrijednosti uz očekivano očuvanje teritorijalnog integriteta. Kako bi država, prema Hobbsovom viđenju društvenog ugovora, ispunila tu obavezu, njezin sistem sigurnosti treba biti organiziran na način da predviđa, upravlja i odgovara na sve oblike rizika i opasnosti. U kontekstu digitalne transformacije sigurnosti, to nije jednostavan zadatak (ako je ikada i bio).

Ipak, sistem državocentrične sigurnosti ne uključuje samo sposobnosti države za očuvanje vrijednosti svojega društva od unutarnjeg i vanjskog ugrožavanja mira i slobode građana, nego i zajedničko djelovanje s drugim društvenim podsistemima radi daljnjeg razvoja društva u cjelini, kao i ljudske civilizacije (Grizold, Tatalović, Cvrtila, 1999). U periodu poslije hladnog rata i sa početkom ere borbe protiv terorizma, korespondira i razvoj tehničkih, tehnoloških, i (u)mrež(e)nih pretpostavki za povećani nadzor. U vezi s tim sam Snowden (2019) piše: „Sudjelovao sam u najznačajnijoj promjeni u povijesti američke špijunaže - promjeni od ciljanog nadzora pojedinaca do masovnog nadzora cijele populacije“ (str. 6). Na osnovu tehnoloških pretpostavki promjene navika ljudi, digitalne transformacije društva i sigurnosti, a pod izgovorom razvoja i zaštite nacionalne sigurnosti, proporcionalno dolazi do ograničavanja

prava i sloboda građana, ali i ugrožavanja same demokratije (Romano, 2011, str. 159-160; Agamben, 2005; Snowden 2019).

No, da se vratimo osnovama ljudskih potreba i vrijednosti, koji bi trebali biti predmetom zaštite. Težnja za dobrobiti, dobrim životom i životom dostojnim čovjeka sastavni je dio ljudskog postojanja (vidjeti i: Tsirogianni, Sammut, Park, 2014). Poznata Maslowljeva teorija hijerarhije potreba (1943) polazi od pretpostavke da ljudi zadovoljavaju svoje želje i potrebe određenim redoslijedom, pa ih je moguće tako hijerarhijski i definirati i postaviti. Maslow (1987, str. 35-58) navodi da individualno ponašanje ovisi o želji da čovjek zadovolji jednu ili više od svojih pet općih potreba: (a) fiziološke, (b) sigurnosne (*safety)*, (c) socijalne, (d) poštovanje samoga sebe, (e) samoostvarenje. U načelu, navedene potrebe hijerarhijski su složene od nižih (fizioloških) prema najvišim (samoostvarenje). Odmah poslije osnovnih fizioloških potreba, slijedi potreba za sigurnošću *(safety)*, kao temeljna psihološka potreba. To Maslow objašnjava kao potrebu za stalnošću, redom, za sigurnosti (*safety*), stabilnosti, ovisnosti; zaštitom; za slobodom od straha, od tjeskobe i haosa, odnosno, kao potrebu za strukturom, poretkom, zakonom, ograničenjima, itd. Digitalna transformacija društva i sigurnosti dodatno usložnjava stvari, daje svoju dozu kompleksnosti. Hibert (2017), uz dozu ironije, dodaje i potrebu za WiFi (spojenošću na Mrežu) i Bateriju (stalni rad pametnih umreženih uređaja) kao još bazičnije potrebe, možemo reći i kao digitalnu realnost Maslowljeve hijerarhije. Međutim, i za ta dva dodatna elementa sigurnost se (i eng. safety i eng. security) opet sama nameće. Da je pristup WiFi uvijek dostupan, siguran, pouzdan, te da su uređaji jednako *safe and secure,* po principima informacijske (u širem smislu) i cyber (u užem smislu) sigurnosti.

U kontekstu vrijednosti i potreba, digitalna transformacija društva, a posebno digitalna transformacija sigurnosti, uzrokovala je neminovne promjene koje su se desile, a za koje još uvijek nismo definisali ili tek trebamo definisati naš pristup i odgovor. Kako i ko definiše društvene vrijednosti? Jedna od širih definicija navodi da „pod društvenim vrijednostima nazivamo društveno kolektivna uvjerenja i sisteme vjerovanja koja djeluju kao vodeća načela u životu“ (Tsirogianni, Gaskell 2011, str. 2). Danas već, samu potrebu za sigurnošću (ali i za potrebama iz sfere društvenog i političkog) ne generišemo iz naših direktnih opažanja već kroz politički konstrukt uvjetovan algoritnima, umjetnom inteligencijom (AI) i tehnokapitalizmom. „Nekada smo digitalne usluge smatrali besplatnima, a sada nas kapitalisti nadzora smatraju besplatnima“ (Zuboff, 2019). Obični građanin u demokratskom društvu zamijenio je svoju ulogu suverena u (ponovnom) uspostavljanju digitalnog društva (i ugovora) s novim ulogama: korisnik usluge, potrošač, proizvođač (besplatnog sadržaja), i kao roba (podaci i pažnja).

Snowden u svojoj knjizi „Trajni zapis“ (2019) objašnjava kao su tvrtke shvatile da se ljudska veza koju je internet omogućio, može unovčiti: „Ovo je bio početak kapitalizma nadzora i kraj interneta kakav sam poznavao"(str.14). Autor dodatno obrazlaže (novi) poslovni model e-trgovina koje su propale jer nisu mogle pronaći ništa što nas zanima: imali su novi proizvod za prodaju, a „taj smo novi proizvod bili mi“ (Snowden, 2019, str. 14). Hibert (2020) objašnjava kako

> „ekstrakcija kognitivnog viška vrijednosti iz neprekidnog živog kapitala (Lazzarato, 2014), mrežnih aktivnosti korisnika, ostvaruje se kroz neprestano bilježenje i praćenje, ali i modifkaciju ponašanja, raspoloženja i navika. Proces razotkrivanja akumulacije i upravljanja tzv. „bihejvioralnim viškom“ (Zuboff, 2019) (matematičkim modelima koji aproksimiraju ljudsko ponašanje algoritamskom modulacijom matrica podataka) počiva na istraživanjima koji ukazuju u kojoj mjeri su naše odluke izložene modelima destabilizacije javne svijesti: „Facebook defnira ko smo, Amazon defnira šta želimo, Google defnira šta mislimo“ (Dyson, 2012, str. 308). Internet je mračna šuma, mentalni

prostor mjesečarenja koji su zaposjele mašine sa kojima postajemo neurološki intimni (Konior, 2020).“ (Hibert, 2020, str. 96)

Možemo dodati da onaj koji ima pristup i mašinsku moć obrade našim meta-podacima, taj može određivati i naš osjećaj sigurnosti, uslovljavajući time sferu političkog, odnosno, može otupiti naša čula i stoga onemogućiti realno sagledavanja rizika, prijetnji, pa i same demokratske realnosti.

Zahvaljujući algoritmima i AI, velike su tehnološke kompanije napravile imperiju i postale novi *gatekeeperi*. Ovog obrta, uglavnom, građani nisu svjesni, drugim riječima, uglavnom ne poznaju kako ti algoritmi rade i kako im oni uređuju svakodnevnicu. Jedno od uobičajenih opravdanja jest da algoritam predstavlja poslovnu tajnu, tj. intelektualno vlasništvo (za npr. Google, Amazon i Facebook, precizno skrojeni algoritmi vrijede stotine milijardi dolara). Može se reći da „*oružja matematičkog uništavanja* (WMD eng. Wepons of Math Distruction - O'Neil 2016) su, prema dizajnu, neprocjenjive crne kutije. Zbog toga je dodatno teško definitivno odgovoriti na drugo pitanje: radi li model protiv interesa subjekta? Ukratko, je li to nepravedno? Oštećuje li ili uništava živote?“ (O'Neil 2016, str. 30).

Šta su u suštini algoritmi? U matematici pojam „algoritam“ znači jednoznačan postupak rješavanja zadane klase problema. Ovdje, u našem kontekstu, „algoritam“ bi trebalo determinirati više kao „automatizirani algoritam“, tj. postupak koji se koristi za automatizaciju obrazloženja ili procesa donošenja odluka i koji, obično, provodi kompjuter upravo s ciljem da se automatizacija i sistemski realizira mnogo većim brzinama od onih koje može postići čovjek; time se, također, automatski pokreću i mnogi drugi postupci. (Whittlestone, et al, 2019, str. 7)

Kao sastavna komponenta algoritama potrebna je „umjetna inteligenciju“ (AI) koju je najteže definirati i čija je definicija stoga najspornija. Ovdje se AI odnosi „na bilo koju tehnologiju koja izvodi zadatke koji bi se mogli smatrati inteligentnima (…) i često se može koristiti za optimizaciju procesa i može se razviti za autonomno djelovanje, stvarajući složena ponašanja koja prelaze ono što je izričito programirano“ (Whittlestone, et al, 2019, str. 7). AI i algoritni uče od ljudi, a za potrebe vlasnika digitalnog kapitala.

Može se stoga reći da je za nešto više od polovine populacije na planeti (63.2%)[13], koja spada u umreženi svijet, stvoreno okruženje u kojem svakodnevno iskustvo postojanja biva oblikovano prisustvom umjetne inteligencije, pri čemu su „algoritmi njegovi gradivni organizacijski elementi“ (Hibert 2020). Treba napomenuti da svi mi, Homo Sapiensi, hranimo algoritme, umjetnu inteligenciju i omogućavamo mašinsko učenje putem našeg digitalnog traga (i rada), interakciju sa IoT (Internet of Things) i svim mogućim korelacijama čovjeka i mašine.

4. Digitalna transformacija sigurnosti

Digitalna transformacija sigurnosti dešava se praktično na svim nivoima: strateškom, operativnom, taktičkom i, naravno, tehničkom. Svaki nivo se može sagledavati iz više uglova, konceptualnih i formalno-pravnih: vojni, policijski, društveni i građanski pristup, zatim kiberdelikvencija, obavještajno-sigurnosno djelovanje u cyber prostoru, potom primjena na javne i privatne institucije, državni nadzor na Mrežom i građanima, digitalna transformacija/ugrožavanje/razvoj ljudskih prava, sigurnosno propitivanje korelacije pojedinca i sigurnosti u cyber prostoru, pa sve do upravljanja nuklearnim potencijalom. Tako širok dijapazon svega što digitalna transformacija sigurnosti obuhvata ili pokriva, zahtijeva

[13] Vidi: https://www.internetworldstats.com/stats.htm (pristup 01.12.2020.)

svakako i sveobuhvatnu ili barem sveobuhvatniju definiciju onoga što sigurnost uistinu jeste u digitalnom prostoru. Dakle:

> „Cyber sigurnost jest stanje i praksa zaštite infrastrukture, informacijsko-komunikacijskih sistema, mreža, uređaja i informacija od ugrožavanja, u cilju zaštite ljudi, materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države i međunarodnih odnosa. Prijetnje kojima se suprotstavlja cyber sigurnost, jesu brojne, ali ih je, radi jednostavnijeg razumijevanja, potrebno posmatrati prije svega kao cilj ili kao sredstvo (1) u cyber kriminalitetu, (2) u politički motivisanim cyber napadima i (3) u cyber terorizmu.“ (Vajzović, 2019, str. 534)

Iako bi bilo znanstveno i zanimljivo i značajno analizirati sve spomenute segmente, ovdje ćemo se ipak fokusirati samo na pojedinca, utopijski viđenog kao aktivnog, konstruktivnog građanina, *perpetuum mobile* demokratskog diskursa i vrijednosti. Digitalna transformacija sigurnosti implicira ne samo korištenje novih tehnologija, mreže, metapodataka, podataka, AI i algoritama za vojne i odbrambene potrebe i za policijski rad, nego uključuje i način na koji sigurnost percipiraju građani, te kakve implikacije ona ima na demokratske procese.

Utopijski, utilitaristički gledano: život dostojan čovjeka, ljudska prava i slobode, dugoročni mir i društvene vrijednosti jesu primarni predmet zaštite. O razumijevanju društvenih vrijednosti u kontekstu pitanja o kojima se ovdje govori, Darvin Lisica (2011a) kaže sljedeće:

> „Temeljne društvene vrijednosti su temeljna uvjerenja, ideje i stanja o onome šta je važno, dobro i poželjno, o čijem prihvaćanju postoji konsenzus unutar određene društvene grupe ili društva u cjelini. One usmjeravaju ponašanje i omogućavaju interakciju pojedinaca i grupa, oblikuju individualne i kolektivne stavove, pomažu profiliranju zajedničkih interesa i ciljeva, osiguravajući tako unutarnju koheziju i stabilnost društvenih struktura kao neophodnih preduvjeta za izgradnju efikasnog sigurnosnog sistema“. (str. 23)

Sam pojam, razumijevanje i doživljavanje sigurnosti (što objektivno, što subjektivno) oduvijek je bilo podložno različitim interpretacijama, zavisno od vremena, geopolitičkog i društvenog konteksta, kao i shvatanja ili mogućnosti objektivnog detektovanja sigurnosnih rizika.

Iako je pojedinac uvijek bio značajan element u planiranju sigurnosti države i društva, treba naglasiti da je to u kontekstu digitalne transformacije sigurnosti, i dodatno došlo do izražaja, i ti na svim razinama: (1) državnom, (2) korporativnom i (3) individualnom, dakle kao kapacitet demokratskog diskursa, kao očuvanje narodnog suvereniteta, ali i kao samozaštita i otpornost na informacijsko-komunikacije distorzije.

(1) Državnu / nacionalnu sigurnost, u kontekstu individua u digitalnom okruženju, sagledavamo u više dimenzija: otpornost pojedinca, kao integralnog djela društva i javnosti na hibridne asimetrične prijetnje i specijalne ratove kroz dezinformacije, manipulacije informacijama, (digitalno)medijske napade na progresivne snage, kao i otpornost na radikalizaciju, nasilni ekstremizam i regrutaciju za potrebe terorizma, osobito putem društvenih mreža.

U dokumentu *Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini* (2019) navodi se da je razvijanje svijesti o cyber sigurnosti i obrazovanje u toj oblasti značajan i integrativni element za sve ostalo. Isto je, također, jasno navedeno u cilju C, C1 i C2. Tu se još potvrđuje i značaj razvoja „šestog čula“ – MIP, gdje se naglašava: „Podržavati procese uključivanja medijske i informacijske pismenosti u formalno i neformalno obrazovanje.“, te „Uvoditi teme vezane za cyber sigurnost i medijsku i informacijsku pismenost u nastavne planove svih nivoa obrazovanja.“ (OSCE 2019, str. 13-14)

U širem kontekstu gledano, Beridan (2008) navodi da strukturu sistema nacionalne sigurnosti u osnovi čine: *funkcije*, *snage* (nosioce), *djelatnosti* (aktivnosti) i *mjere* sistema sigurnosti. Medijsku i informacijsku pismenost (MIP) možemo najjednostavnije pozicionirati kao komponentu Snaga (nosilaca) sistema sigurnosti, pod segmentom „Društvo i njegove komponente". MIP bi, kao osnažen element, mogao značajno doprinijeti da u perspektivi jedno društvo (neko, svako) bude ili postane mnogo sigurnije (zaštićenije) od vanjskih i unutrašnjih neprijatelja i napada. Prirodno pravo svakog ljudskog bića i skupine kojoj ono pripada, jest pravo na „samoodbranu, samozaštitu i samopomoć" (Grizold, Tatalović, Cvrtila 1999, str. 11), ali je za sve to potrebno da čulno zabilježimo i shvatimo opasnost, što je u svijetu „algoritamskih kapija" (Hibert 2020) vrlo izazovno. Sun Tzu u vezi s tim pitanjima podsjeća da svako vođenje rata počiva na obmani, ali istovremeno naglašava da se najveći uspjeh ne sastoji od toga da pobijedimo neprijatelja u svim bitkama, već da otpor neprijatelja savladamo bez borbe (Sun, Nylan, 2020).

Kad je riječ o specijalnim operacijama, one u izučavanjima polemologije[14] i vojnih doktrina, nisu novina. One predstavljaju skup organiziranih aktivnosti i djelovanja koje određena država ili više njih poduzimaju (a) *u miru* (u političkom, ekonomskom, vojnom, medijskom, kulturnom, naučnom i svakom drugom pogledu) - radi slabljenja stabilnosti neke države, naročito njezine stabilnosti u pružanju otpora, odnosno, (b) *u ratu* – radi slabljenja njezine sposobnosti za odbranu, čime se ta (neka) država dovodi u određeni stepen zavisnosti i potčinjenosti.

Specijalne operacije uključuju i prijeratna, i ratna i poratna događanja, ali u pravilu bez obostranog i masovnog korištenja vojne sile. Njihov osnovni cilj jest slabljenje određene države ili političke zajednice, tj. njene unutarnje i spoljne politike, slabljenje njezinoga otpora neprijateljskoj politici i, da ponovimo, njezino dovođenje u ovisan i potčinjen položaj. Načelno, specijalne operacije podrazumijevaju političke, vojne, ekonomske i druge djelatnosti protiv jedne države ili grupe država, što osim obavještajnih aktivnosti, uključuje i različita druga djelovanja: psihološko-propagandna, subverzivna, odbrambena (Molander et al., 1996; Beridan, 2008; Moffat, 2006; Beridan, Tomić, Kreso, 2001). Promatramo li pak sve to u kontekstu društvenih mreža i online platformi, možemo se složiti da su specijalne operacije, praktično, „strateško polje biopolitičke moći u kojem se kao centralna karika pojavljuje mrežni pojedinac zapleten u mrežu bihejvioralnog inžinjeringa" (Hibert, 2020).

Ono što je zanimljivo za dalja istraživanja, jesu modeli, pojavni oblici, efikasnost i elementi hibridnih asimetričnih specijalnih operacija, jer razvoj interneta, cyber prostora i Mreže otvara gotovo neiscrpne nove mogućnosti. Tako Snowden (2019) navodi da njegova generacija nije samo unaprijedila obavještajni rad, već su išli i korak dalje: „u potpunosti smo redefinirali što jeste obavještajni posao. Za nas to nisu bili tajni sastanci ili tajna predaja informacija, već rad sa podacima" (str. 8). On pritom vrlo slikovito opisuje protuustavna djelovanja obavještajnih agencija i narušavanje osnovnih vrijednosti svakog slobodnog društva: „Sjedio sam za kompjuterskim terminalom s kojeg sam imao praktički neograničen pristup komunikacijama gotovo svakog muškarca, žene i djeteta na zemlji koji su ikad koristili telefon ili dodirivali računalo. Među tim ljudima bilo je oko 320 milijuna mojih sugrađana Amerikanaca, koji su u redovnom svakodnevnom životu bili pod nadzorom" (str.10).

Strateška promišljanja, vjerovatno najcitiranijeg autora iz ove oblasti Sun Tzua, autorica Michael Nylan (2020) u uvodu najnovijeg prijevoda ovog klasika, kontekstualizira današnjicu naglašavajući značaj ovoga djela „posebno u doba kada veliki podaci (*eng. big data*) i umjetna inteligencija sugeriraju da su ljudi kao vrsta podatniji (prijemčiviji za oblikovanje) nego što

[14] grč. Polemeo -borim se, ratujem + logos- riječ, govor, pojam, misao, razum) naučno, znanstveno istraživanje rata kao društvene pojave, njegovih uzroka, ciljeva i posljedica.

bismo željeli misliti, dok se internet sve više vidi kao neprijateljski svijet prepun novih ratišta“ (str. 19-20). S druge strane, kroz *doktrinu šoka* (Klein 2008) demokratsko društvo je u krizi jer su građani previše rastrojeni (emocionalno i fizički) da bi se uključili i razvili adekvatan odgovor, te se učinkovito opirali kontroverznim i upitnim politikama koje javne vlasti usvajaju. Demokratski deficit koji se stvara progresivno, negativno djeluje na stanje sigurnosti u jednom društvu, pogotovo imajući u vidu da se vlasti sve više integrišu sa velikim tehnološkim kompanijama kojima se prenose zadaci (*outsourcing*), često uz ovlasti i visoku cijenu, mnogih njihovih osnovnih funkcija na privatne (tehnološke) kompanije (Klein 2020).

(2) Posmatrano iz ugla *korporativnog* nivoa, u vremenu kad su informacije najvrjedniji resurs, kad je informacija (tj. podatak/data) postala vrjednija i od nafte (Economist, 2017; 2010) - informacijska sigurnost postaje ključna za osiguravanje poslovnog kontinuiteta, zaštitu podataka, imovine, sigurnost mreže, za upravljanje incidentima, zaštitu privatnosti itd. Jer, sistemom informacijske sigurnosti obuhvataju se „fizička lica, procesi, organizacija i tehnologija. Taj sistem se sastoji od uravnoteženog skupa sigurnosnih mjera, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacionih sistema, koordiniranog uvođenja formalnih procedura, kao što su procjene rizika, certificiranje uređaja i akreditacije tehničkih sistema za primjenu u određenim segmentima poslovnih procesa u Institucijama.“ (Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, 2017).

Uz ostale, najznakovitija je možda ISO 27000[15] porodica standarda, koja se, uprkos pravilima i procedurama, ipak zasniva na visokom nivou pojedinačne svijesti o sigurnosti i njenim elementima. Cyber sigurnost, kao poddomen informacijske sigurnosti, oslanja se na tri stuba: (1) hardware/software, (2) procedure i (3) ljudski resursi. Budući da je *čovjek* tradicionalno najslabija karika u lancu, ključno je, kao preduslov za visok stepen zaštite, da on bude visoko osviješten, obučen, medijski i informacijski pismen. Svijest o informacijskim i cyber prijetnjama prvi je i najvažniji korak u postizanju sigurnosti. Nakon toga korisnik može biti spreman za borbu protiv takvih prijetnji, pri čemu treba imati na umu da sigurnost nije jednokratni mehanizam već je to kontinuirani proces. (Calder, Watkins, 2015; Chopra, Chaudhary, 2020; Prasad, 2020; Vajzović, 2019).

(3) Na *individualnom* je nivou zanimljiva percepcija kako u svakodnevnom životu (globalno) o sigurnosti i miru brine država, dok individualna sigurnost (safety) očigledno jest ili bi trebala biti osobna briga (Farnicka 2017). Čini se, međutim, da smo sve svjesniji (ili možda baš i nismo?!) potrebe za samozaštitom u digitalnom okruženju, da sve više razumijevamo značaj digitalnog traga, privatnosti u cyber prostoru, samosvijest o funkcionisanju i utjecaju društvenih mreža. Razumijevanje *backend*[16] nevidljivog dijela Mreže, algoritmi i AI, te njihov utjecaj na demokratske procese, ljudska prava, političku komunikaciju, i očuvanje osnovnih principa ljudskih prava i sloboda - samo su neki od izazova na kojima pojedinac (idelano!) treba svakodnevno raditi u pravcu shvatanja i svoga prilagođavanja, pozicioniranja i djelovanja (vidjeti: Rašidović, 2012). U tom pogledu su danas možda i najzahtjevniji procesi upravo u sferi (vjerovatno) najizraženijeg čovjekovog instinkta, a to je zaštita vlastitih potomaka i porodice. Segment zaštite, tj. „opismenjavanja“ djece vezano za njihovu interakciju i djelovanje na Mreži, predmet je posebnih multidisciplinarnih istraživanja. Pravi omjer prednosti i mogućnosti digitalnog svijeta za dijete naspram nedostataka, prijetnji i rizika – jest nešto što se teško može precizirati.

[15] Za više vidi: ISO 27000 porodica standarda: https://www.iso.org/search.html?q=27000

[16] *Eng*. U softverskom inženjerstvu izrazi frontend (prednji) i backend (stražnji) kraj odnose se na razdvajanje problema između prezentacijskog sloja (prednji kraj) i sloja pristupa podacima (stražnji kraj) dijela softvera ili fizičke infrastrukture ili hardvera. Klijent se obično smatra prednjim krajem, a poslužitelj obično stražnjim krajem.

U tom bi se pravcu možda mogla povući nekakva paralela sa doktrinom bivše SFR Jugoslavije u pogledu uvođenja u obrazovni sistem nastavnog predmeta „Opštenarodna odbrana i društvena samozaštita“ (ONO i DSZ). Ideja je, kako navode neki autori, između ostalog bila da se odbrambena strategija uskladi sa jugoslavenskom ideologijom samoupravnog socijalizma (doktrine o "naoružanom narodu"), poticana svakako strahom od kakve potencijalne invazije (Stevanović 2018). Na sličan bi način, recimo, manje ili više, MIP trebao razviti preventivno set kompetencija kod učenika, samo ovaj put u digitalnom okruženju. Poenta je razvoj otpornosti na sigurnosne prijetnje u određenom prostoru (cyber) i vremenu (sada i sutra), sa svim pratećim izazovima digitalne transformacije sigurnosti u algoritamskoj demokratiji.

Gledajući sa strateškog nivoa, u smislu ratovanja, jasno da je puno efikasnije, efektivnije, izvodljivije i održivije napasti neko područje, pokoriti ga i vladati nekom državom ili nekim narodom bez upotrebe konvencionalne vojne snage. Tradicionalni domeni ratovanja (kopno, zrak, voda i svemir), koji su također tehnološki vrlo sofisticirani i digitalno transformirani, značajno osnaženi algoritnima i AI - u budućnosti će (vjerovatno) biti neka vrsta preventivne snage u pričuvi za slučaj da treba pokazati i omjer snaga u fizičkom svijetu. No, kako se većina društvenih, političkih, poslovnih i ličnih aspekata života seli ili paralelno odvija u cyber prostoru, na Mreži (baš kao i djelimična fuzija tradicionalnih domena i cyber ratovanja) - potrebno je sagledati tko tim prostorom vlada i gdje se u svemu tome nalazi narod, koji u demokratskom društvu i jest nosilac suvereniteta. Većina sigurnosnih prijetnji i ratovanja se (već) odvija u sferi Interneta, cyber prostora, Mreže i Logosa. „Osjetljivost građana (pa i cijelog društvenog sistema) na hibridne asimetrične distorzije i napade (vanjske i unutrašnje) proporcijalno se povećala, te su i izazovi za sigurnost postali značajniji“ (Vajzović 2019).

Sama suština demokratske filozofije uređenja društvenih odnosa, dakle univerzalnost ljudskih prava i sloboda, dovodi se u pitanje upravo upotrebom nevidljivih sila mreže – algoritama i umjetne inteligencije (vidjeti: Crawford i Joler 2018; Perkov 2017a; 2017b; 2017c). Zato se nameću i vrlo važna pitanja koja se ne postavljaju dovoljno često: u čijem su vlasništvu te „sile“ i za koga rade; ko ima „legitimni“ aparat za prisilu (a to više nije samo prisila u fizičkom svijetu); koliko narod nad njima ima demokratski nadzor i kontrolu?

Važno je naglasiti da „ideal informisanog i obrazovanog aktivnog građanina jest osnov demokratske utopije društva koje teži prosperitetu, visokom stepenu ostvarivanja ljudskih prava i sloboda, životu dostojnom čovjeku i sve to u mirnom i sigurnom okruženju. Takav ideal implicira građanina koji ima razvijeno kritičko mišljenje i otpornost na manipulacije (primarno političko-ekonomske), unutrašnje i vanjske. Takvo društvo ima pretpostavke da je izraz slobodne volje čovjeka, da je autonomno razvijen i realizovan kao izraz nosioca suvereniteta u demokratskom društvu kojem je zagarantovana sigurnost.“ (Vajzović 2019, str. 530; vidjeti i: Zgodić, 2010). Na taj se način život modernih informacijskih društava sve više integriše u cyber prostor, a samim time i sigurnosni izazovi sve više proizlaze iz tog istog domena. Ima li se to na umu, jasno će biti zašto se otpornost jednoga društva, države, političkog, ekonomskog i sigurnosnog sistema, medijska i informacijska pismenost sve očitije percipira kao jedna od ključnih kompetencija - i svakoga građanina pojedinačno i društva u cjelini. Odnos pojedinca prema vlastitoj i grupnoj (kolektivnoj) sigurnosti se usložnjava kada građanin postaje *umreženi građanin*, te (ne)svjesno postaje korisnik digitalnih platformi i usluga, kreator sadržaja i njihov konzument, te u konačnici proizvod i predmet trgovine, ali i izmanipulirani objekt unutar algoritamske demokratije (vidjeti: Amer 2019, Rhodes, l. , Orlowski, J., 2020; McDavid, Jodi, 2020). Možemo reći da „iz proklamiranog društva znanja stigli smo u društvo podataka, sačinjeno iz korisnički generiranih, remiksovanih sadržaja postčinjenične naravi. (…) karakter današnje hegemonije temelji se na informacijskom višku o podacima (metapodaci), a ne deficitu znanja (pristup informacijama)“ (Hibert, 2020, str. 97).

5. Zaključak

Sam historijski tok odslikan u industrijskom i tehničko-tehnološkom napretku ne mora sam po sebi značiti i društveni prosperitet, a savremeni razvoj može u sigurnosnom smislu biti velika opasnost, te u isto vrijeme i velika šansa za čovječanstvo i čovjeka kao pojedinca, pod uvjetom da se adekvatno i pravovremeno uspostave kontrolno-sigurnosni mehanizmi koji bi vodili ljudskom prosperitetu i pogodovali zajednici. Dobar put ka ostvarenju toga bilo bi etičko, političko, pravno, pa i sigurnosno promišljanje tehnologije, AI, algoritama i tehnoloških kompanija, ali stvaranje pretpostavki za razumijevanje značaja i same paradigme algoritamske demokratije. Na tim pretpostavkama ovaj rad kroz antidisciplinarni pristup kritičkim sigurnosnim studijama utvrđuje temeljnu ulogu medijske i informacijske pismenosti u osnaživanju i jačanju otpornosti građana kao ključnih snaga sigurnosti: i kao pojedinaca u tradicionalnim segmentima snaga sigurnosti (oružane snage, policija, itd), ali i kao zasebnog elementa snaga sigurnosti: „Društvo i njegove komponente“ (Beridan, 2008) koji sve više preuzimaju ulogu gatekeepera u digitalnom društvu informacijskog nereda (information disorder).

Ta i takva demokratija (algoritamska) mora biti i ostati u rukama i pod kontrolom građana kao nosilaca suvereniteta (recimo kroz ideju i pokret za zajednička dobra – *eng. Commons movement*[17]) (Tomašević, 2018). Ostaje jednako važno osnažavanje građana putem obrazovanja, te podizanje nivoa medijske i informacijske pismenosti u stanju post-demokratije[18] i digitalnog (Stalder, 2018; Carlsson, 2019; Smith, T. G. 2017, str. 1-9). Medijsku i informacijsku pismenost kao šesto čulo posebno je značajno za razumijevanje digitalne transformacije društva i sigurnosti, te njihove implikacije na demokratski diskurs i njihove povezanosti sa prijetnjama, rizicima i sigurnosti na državnom, korporativnom i individualnom nivou: kao kapacitet demokratskog diskursa, kao očuvanje narodnog suvereniteta, ali i kao samozaštita i otpornost na hibridne asimetrične sigurnosne prijetnje. Medijska i informacijska pismenost u savremenom trenutku neophodan je i poželjan elemenat shvatanja, kreiranja i zaštite sigurnosti pojedinca, organizacije, države i (post)demokratije!

Bibliografija:

1. About the Commons: On the Commons. http://www.onthecommons.org/about-commons.
2. Agamben, Giorgio (2005) State of Exception, trans. Kevin Attell. Chicago: University of Chicago Press.
3. Amer, K., Noujaim, J. & Amer, K., Barnett, E., Kos, P. (2019) The Great Hack. SAD [Video file]. Dostupno na: https://www.netflix.com/title/80117542
4. Amoore, L. (2009) ‘Algorithmic War: Everyday Geographies of the War on Terror’, Antipode, 41: 49–69.
5. Anderson, K. (2008, August 28). Apomediation: Word of the Day. Retrieved December 1, 2020, from https://scholarlykitchen.sspnet.org/2008/08/28/apomediation-word-of-the-day/
6. Beridan, I. (2008) Politika i sigurnost. Fakultet političkih nauka, Sarajevo.
7. Beridan, I., Tomić Ivo M., & Kreso, M. (2001). Leksikon sigurnosti. "DES".
8. Bosančić, B. (2017). DIKW – hijerarhija: za i protiv. Vjesnik bibliotekara Hrvatske, 60 (2-3), 1-24. Preuzeto s https://hrcak.srce.hr/195861

[17] Vidi: http://www.onthecommons.org/about-commons#sthash.ujNneYrn.dpbs

[18] Stadler (2018, viii) taj termin "post-demokratija" koristi „jer proširuje mogućnosti, pa čak i zahtjeve za (ličnim) sudjelovanjem, dok se sve veći aspekti (kolektivnog) odlučivanja premještaju u arene koje su strukturno odvojene od participacije. Zapravo, ta arena stvaraju autoritarnu stvarnost u kojoj je mala elita uvelike ovlaštena na štetu svih ostalih.“

9. Brahmachary, A. (2019, May 04). DIKW Model: Explaining the Concept of DIKW Hierarchy in ITIL. Retrieved December 19, 2020, from https://www.certguidance.com/explaining-dikw-hierarchy/
10. Calder, A., & Watkins, S. (2015). IT governance: an international guide to data security and ISO 27001/ISO 27002. KoganPage.
11. Carlsson, U. (ur.) (2019) Understanding Media and Information Literacy (MIL) in the Digital Age A Question of Democracy. (UNESCO) Department of Journalism, Media and Communication (JMG), University of Gothenburg
12. Cavelty, M. D., & Balzacq, T. (2017). Routledge handbook of security studies. Abingdon, NY, N.Y.: Routledge.
13. Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System: Security Management Based on Iso 27001 Guidelines. Apress L.P.
14. Clausewitz, C. V., & Howard, M. (1993). On war. Carl von Clausewitz. London: David Campbell.
15. Collective, C. (2006). Critical Approaches to Security in Europe: A Networked Manifesto. Security Dialogue, 37(4), 443-487. doi:10.1177/0967010606073085
16. Crawford, K and Joler, V. (2018) Anatomy of an AI System: The Amazon Echo As An Anatomical Map of Human Labor, Data and Planetary Resources. AI Now Institute and Share Lab, (September 7, 2018) https://anatomyof.ai
17. Dujović, J. (2006) Rukovođenje i upravljanje sistemima sigurnosti. Sarajevo: FPN
18. Eysenbach, G. (2008). *Credibility of Health Information and Digital Media: New Perspectives and Implications for Youth*. In M. J. Metzger, & A. J. Flanigan (Eds.), Digital Media, Youth, and Credibility (pp. 125-154). Cambridge, MA: MIT Press.
19. Farnicka, Marzanna. „Impact of Cyberspace on Individual Safety and Group Security—A Human Developmental Psychology Approach“ (95-117), in Ramírez, J. M., García-Segura, L. A., & Medina, C. G. L. (2017). Cyberspace: risks and benefits for society, security and development. Springer.
20. Ferrajoli, L. „Ustavna demokratija“, Revus [Online], 18 | 2012, Online since 14 September 2013, connection on 21 December 2020. URL: http://journals.openedition.org/revus/2303; DOI: https://doi.org/10.4000/revus.2303
21. Foucault, M. (2002) 'Society Must Be Defended': Lectures at the Collège de France, 1975–76, trans. David Macey (New York: Picador).
22. Foucault, M. (2007) Security, Territory, Population: Lectures at the the Collège de France (Basingstoke: Macmillan).
23. Graham-Harrison, E., & Cadwalladr, C. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved December 21, 2020, from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
24. Greenfield, A. (2013). Against the Smart City. London, UK: Verso.
25. Grizold, A., Tatalović, S., Cvrtila, V. (1999) Suvremeni sistemi nacionalne sigurnosti. Fakultet političkih znanosti; Hrvatska udruga za međunarodne studije
26. Guha, M. (2011). Reimagining war in the 21st century: From Clausewitz to network-centric warfare. London: Routledge.
27. Gunkel, D. J. (2014). Social Contract 2.0 : Terms of Service Agreements and Political Theory. Journal of Media Critiques, 1(2), 145-168. doi:10.17349/jmc114208
28. Hibert, M (2017) LIFE THAT WASN'T THERE: OGLED O NEVIDLJIVOSTI. Izlaganje na Vaša(r) ideja. Dostupno na: https://www.youtube.com/watch?v=smbN1NnpSQc
29. Hibert, M. (2018) Digitalni odrast i postdigitalna dobra: krtičko bibliotekarstvo, disruptivni mediji i taktičko obrazovanje. Zagreb. Multimedijalni institut i Institut za političku ekologiju. Dostupno na: http://ipe.hr/wp-content/uploads/2019/01/Mario_Hibert-Digitalni_odrast.pdf
30. Hibert, M. (2020). Mediji i društvena pismenost (91-116) u Jasmina Husanović, Damir Arsenijević i Mario Hibert (2020). Društvena pismenost: kultura, ekologija, mediji. Muzej književnosti i pozorišne umjetnosti; Front Slobode
31. Hobbes, T. (2009). Leviathan: By Thomas Hobbes. The Project Gutenberg EBook.

32. *Hrvatska enciklopedija, mrežno izdanje*. Leksikografski zavod Miroslav Krleža, 2020. Informacijska i komunikacijska tehnologija. Pristupljeno 01. 12. 2020. https://www.enciklopedija.hr/natuknica.aspx?id=27406
33. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2020. Pristupljeno 01. 12. 2020. http://www.enciklopedija.hr/Natuknica.aspx?ID=37001
34. Ito, J. (2018). Practice of Change Doctoral dissertation. Keio University. Retrieved from https://www.practiceofchange.org/
35. Jacobs, G., Bayerl, P., Horton, K., & Suojanen, I. (Eds.). (2021). International Security Management New Solutions to Complexity. Cham: Springer International Publishing.
36. Kapitzke, C. (In)formation literacy : a positivist epistemology and a politics of (out)formation. // Educational theory. Vol. 53, 1 (2003). URL: http://eprints.qut.edu.au Pristup: 1.12.2020.
37. Klein, N. (2008). The shock doctrine the rise of disaster capitalism. Picador: New York.
38. Klein, N. (2020, May 08). Under Cover of Mass Death, Andrew Cuomo Calls in the Billionaires to Build a High-Tech Dystopia. Retrieved December 1, 2020, from https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shock-doctrine/
39. Krause, K., Williams, M. C. (1997). Critical security studies: Concepts and cases. London: Routledge.
40. Kulenović, F. Strategies of Apomediation in Complex Information Surounding, Abstract. 15. juni 2018. Konferencija: LIBRARIES IN THE DIGITAL AGE (LIDA) 2018, University of Zadar, Croatia, 13 - 15 June 2018. Dostupno na: http://lida.ffos.hr/2018/program/ - http://lida.ffos.hr/2018/datoteke/abstracts_2018/LIDA_2018_Kulenovic_paper_68.docx
41. Line, M., Tøndel, I., Nordland, O., & Røstad, L. (2006). Safety vs. Security? (PSAM-0148). Proceedings of the Eighth International Conference on Probabilistic Safety Assessment & Management (PSAM), 1202-1210. doi:10.1115/1.802442.paper151
42. Lisica, D (2011a). *Sigurnosni rizici i temeljne društvene vrijednosti Bosni i Hecegovini* (Vol.1). Sarajevo: Fakultet političkih nauka.
43. Lisica, D (2011b). *Sigurnosni rizici i temeljne društvene vrijednosti Bosni i Hecegovini* (Vol.2). Sarajevo: Fakultet političkih nauka.
44. Lovink, G. (2019). Sad By Design: On Platform Nihilism. London: Pluto Press.
45. Lovink, G., Nazaruk, T. (2018, 14. mart). Interview with Geert Lovink by Taras Nazaruk. Amsterdam: Institute for Network Cultures. Dostupno na: http://networkcultures.org/geert/2018/04/29/social-media-critique-with-geert-lovink-for-the-ukrainian-magazine-korydor/?pdf=1587
46. Mangold, P.(1990) National Security and International Relations, London, Routledge.
47. Masleša, R. (2001). Teorije i sistemi sigurnosti. ISBN: 978-9958-635-10-0
48. Maslow, A. H., Frager, R., Fadiman, J., McReynolds, C., & Cox, R. (1987). Motivation and personality. New Delhi, India: Pearson Education.
49. Maslow, A.H. (1943) A Theory of Human Motivation. Originally Published in Psychological Review, 50, 370-396. Pristup: http://psychclassics.yorku.ca/Maslow/motivation.htm
50. McDavid, J. (2020) "The Social Dilemma," Journal of Religion & Film: Vol. 24 : Iss. 1 , Article 22.Available at: https://digitalcommons.unomaha.edu/jrf/vol24/iss1/22
51. Meyer, T., Hinchman, L. P. (2010). Media democracy: How the media colonize politics. Cambridge: Polity.
52. Moeller, D. P. (2020). Cybersecurity In Digital Transformation Scope And Applications. S.l.: SPRINGER NATURE.
53. Moffat, J. (2006). Complexity theory and network centric warfare. CCRP Publication Series.
54. Molander, R. C., Riddile, A. S., & Wilson, P. A. (1996). Strategic information warfare: a new face of war. RAND.
55. Neocleous, M. (2008). Critique of security. Montreal: McGill-Queen's University Press.

56. Nuhić, M. (2000). Komuniciranje: Od pećinskog crteža do interneta. Sarajevo: FPN Sarajevo. ISBN 9958947633-9789958947636.
57. O'Neil, C. (2016). Weapons of math destruction. How big data increases inequality and threatens democracy. London: Penguin Books.
58. OSCE (2019) Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini. Dostupno na: https://www.osce.org/bs/mission-to-bosnia-and-herzegovina/438386?download=true
59. Peoples, C., Vaughan-Williams, N. (2014). Critical Security Studies: An Introduction. Taylor and Francis.
60. Perkov, B. (01.08.2017.a). Političko-informaciono ratovanje: kratko uputstvo. Dostupno: https://labs.rs/sr/politicko-informaciono-ratovanje-kratko-uputstvo/.
61. Perkov, B. (04.08.2017.b). Nematerijalni rad i prikupljanje podataka. Dostupno: https://labs.rs/sr/nematerijalni-rad-i-prikupljanje-podataka/.
62. Perkov, B. (17.08.2017.c). Istraživanje metapodataka: Haking Tim. Dostupno: https://labs.rs/sr/istrazivanje-metapodataka-haking-tim/.
63. Podumljak, M. (2018) TRUMP'S CODE: Making Money on Populist Disorder. Partnership for Social Development (PSD), Zagreb. ISBN: 978-953-55446-6-1
64. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine. Službeni glasnik Bosne i Hercegovine br. 2017/38)
65. Prasad, R. (2020). Cyber security: the lifeline of information and communication technology. Springer.
66. Ramírez, J. M., & Biziewski, J. (2020). Security and defence in Europe. Cham, Switzerland: Springer Nature.
67. Ramírez, J. M., García-Segura, L. A., & Medina, C. G. L. (2017). Cyberspace: risks and benefits for society, security and development. Springer.
68. Rašidović, E. Beba. 2012. „Informacijska pismenost i sigurnosna kultura mladih", Kriminalističke teme, (3-4), pp. 185-198.
69. Rhodes, l. & Orlowski, J. (2020) The Social Dilemma. [Video file]. Dostupno na: https://www.netflix.com/search?q=social%20dilemma&jbv=81254224
70. Robinson, L., (2013) One Hundred Victories: Special Ops and the Future of American Warfare, New York: Public Affairs ISBN 978-1-61039-149-8
71. Roland, A. (1992). Secrecy, Technology, and War: Greek Fire and the Defense of Byzantium, 678-1204. Technology and Culture, 33(4), 655-679. doi:10.2307/3106585
72. Romano, Silvina M. (2011) Liberal Democracy and National Security: Continuities in the Bush and Obama Administrations, Critical Sociology, 38 (2): 159-178.
73. Rowley, J. (2007). "The wisdom hierarchy: representations of the DIKW hierarchy". Journal of Information and Communication Science. 33 (2): 163–180.
74. Salter, M. B., & Mutlu, C. E. (2013). Research methods in critical security studies: An introduction. London: Routledge, Taylor & Francis Group.
75. Schmitt, M. N. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
76. Shera, J. (1961). Social Epistemology, General Semantics, and Librarianship. (Prev. Gordana Stokić). Wilson Library Bulletin, 35. Dostupno na: https://www.nb.rs/view_∫le.php?∫le_id=489
77. Shera, J. H., & Foskett, D. J. (1965). Libraries and the organization of knowledge / by Jesse H. Shera; ed. and with an introduction by D.J. Foskett. Hamden, CT: Archon Books.
78. Smajić, M., Seizović, Z., Turčalo, S., (2017) Humana sigurnost u postkonfliktnom kontekstu. Fakultet političkih nauka, Sarajevo
79. Smith, T. G. 2017. Politicizing Digital Space: Theory, The Internet, and Renewing Democracy. London: University of Westminster Press. DOI: https://doi.org/10.16997/book5.a. License: CC-BY-NC-ND 4.0
80. Snowden, E. (2019) "Permanent Record". Apple Books.
81. Stalder, F.(2018). The Digital Condition. Newark, SAD: Polity Press.
82. Stevanović, K. (2018, September 3). Srednjoškolci u Beogradu zainteresovani za odbranu i zaštitu. BBC News na srpskom. https://www.bbc.com/serbian/lat/srbija-45359363.

83. Stokić Simončić, G. “Istorija biblioteka kao naučna disciplina“. Glasnik Narodne biblioteke Srbije 2014/15 (2016): 87–95. UDK: 02 (091). Dostupno na: https://www.nb.rs/view_file.php?file_id=4787
84. Sun, W., & Nylan, M. (2020). The art of war. New York, NY: W. W. Norton et Company.
85. The Economist (06.05.2017.) The world’s most valuable resource is no longer oil, but dana: The data economy demands a new approach to antitrust rules. Dostupno na: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
86. The Economist Newspaper. (2010, July 1). *War in the fifth domain*. The Economist. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.
87. The Smithsonian Institution's Human Origins Program. (n.d.). Retrieved December 19, 2020, from https://humanorigins.si.edu/
88. Tomašević, T. (2018). Zajednička dobra u Jugoistočnoj Europi: Primjeri Hrvatske, Bosne i Hercegovine i Sjeverne Makedonije. Zagreb: Institut za političku ekologiju. Dostupno na: https://ipe.hr/publikacije/zajednicka-dobra-u-jugoistocnoj-europi/
89. Tsirogianni S., Sammut G., Park E. (2014) Social Values and Good Living. In: Michalos A.C. (eds) Encyclopedia of Quality of Life and Well-Being Research. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-0753-5_3666
90. Tsirogianni, Gaskell (2011) The Role of Plurality and Context in Social Values
91. Turčalo, S., Smajić, M., Vajzović, E. (2019) “Euro-Atlantic Integration of Bosnia and Herzegovina: Internal Challenges And Foreign Influences”. SECURITY FORUM 2019. Interpolis, Banská Bystrica, Slovakia. Pp. 169 – 175. ISBN 978-80-973394-1-8
92. Vajzović, E. (2016) Medijska demokracija: političko–etički aspekti regulacije sektora komunikacije u procesu evropskih integracija Bosne i Hercegovine. Doktorska disertacija. Fakultet političkih nauka Univerzitet u Sarajevu
93. Vajzović, E. (2017). Informacijsko društvo i demokratija: građanska pismenost za digitalno doba. U D. V. Nedeljković & D. Pralica (Authors), Digitalne medijske tehnologije i društveno-obrazovne promene 7 (pp. 268-278). Novi Sad: Filozofski fakultet, Odsjek za medijske studije. UDC 321.7:004.738.
94. Vajzović, E. (2019). Medijska i informacijska pismenost u sistemu cyber sigurnosti. Kriminalističke Teme, (5), 529-543. Retrieved from http://krimteme.fkn.unsa.ba/index.php/kt/article/view/240
95. Vajzović, E. (ur.). (2020). Medijska i informacijska pismenost: istraživanje i razvoj. Sarajevo: Fakultet političkih nauka. ISBN 978-9926-475-09-3. Dostupno na https://fpn.unsa.ba/b/wpcontent/uploads/2020/12/MEDIJSKA-I-INFORMACIJSKA-PISMENOSTISTRAZIVANJE-I-RAZVOJ_e-izdanje-1.pdf
96. Vajzović, E., Turčalo, S., Smajić, M., (2019) “Collective Cyber Security Defence – Prospects for Western Balkans” SECURITY FORUM 2019. Interpolis, Banská Bystrica, Slovakia. Pp.186-203. ISBN 978-80-973394-1-8
97. Wark, M. (2006). Cyberculture studies: An antidisciplinary approach (version 3.0). In D. Silver & A. Massanari (Eds.), Critical cyberculture studies (pp. 68–78). New York: NYU Press.
98. Whittlestone, J. Nyrup, R. Alexandrova, A.Dihal, K. Cave, S. (2019) Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. London: Nuffield Foundation. Dostupno na: http://lcfi.ac.uk/media/uploads/files/Ethical-and-Societal-Implications-of-Data-and-AI-report-Nuffield-Foundat_tG6yy08.pdf
99. Wolfers, A. (1962) Discord and Collaboration: Essays on International Politics, Baltimore: John Hopkin University Press.
100. Zgodić, E. (2010). Tajni život demokratije. Dobra knjiga. Sarajevo.
101. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs.