Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

MEDIJSKA I INFORMACIJSKA PISMENOST U SISTEMU CYBER SIGURNOSTI

MEDIA AND INFORMATION LITERACY IN CYBER SECURITY SYSTEM

Pregledni naučni rad

Emir Vajzović[488]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Činjenica da se informacijska, komunikacijska, medijska, obrazovna i sigurnosna okruženja mijenjaju, stvara nove mogućnosti i izazove modernim društvima.
Ciljevi rada (naučni i/ili društveni): Kvaliteta primljenih informacija uveliko utječe na naše odluke i postupke koji iz njih slijede, ali jednako predstavlja sigurnosni izazov u kontekstu dezinformacija, utjecaja raznih aktera na demokratske i sigurnosne procese.
Metodologija/Dizajn: Tehnološki napredak podstaknuo je, kvalitativno i kvantitativno, razvoj medija i drugih dobavljača informacija od kojih građani stiču različita znanja i primaju brojne i značajne informacije, uz mogućnost da ih dalje obrađuju i distribuiraju, ali i da donose odluke od sigurnosnog i nacionalnog značaja.
Ograničenja istraživanja/rada: Rad je analizirao relevantnu akademsku literaturu.
Rezultati/Nalazi: Od tri komponente za razmatranje nivoa cyber sigurnosti jedne države: tehnologija, procedura i ljudskih resursa - ovi posljednji (ljudski resursi) predstavljaju možda i najizazovniju komponentu za unapređenje nacionalne sigurnosne politike i doktrine.
Generalni zaključak: Razvoj i podizanje nivoa medijske i informacijske pismenosti postaje nezaobilazno u podizanju nivoa nacionalne sigurnosti, kao i ostvarivanju pravaca i ciljeva postavljenih u strategijama cyber sigurnosti.
Opravdanost istraživanja/rada: Uz digitalnu transformaciju društva, te razvoj novih generacija u digitalnom okruženju - medijska i informacijska pismenost postaje sve važniji element za preispitivanje obrazovnog sistema, cjeloživotnog učenja, demokratskih društava i aktivnog građanstva, ali i cyber sigurnosti svih država.

Ključne riječi

medijska i informacijska pismenost, informacijska i cyber sigurnost, digitalna transformacija društva, nacionalna sigurnost

[488] Docent, Odsjek sigurnosnih i mirovnih studija, Fakultet političkih nauka Univerziteta u Sarajevu. emir.vajzovic@fpn.unsa.ba.

Abstract

Reason for writing and research problem (s): The information, communication, media, educational and security environments are changing which is also creating new opportunities and challenges for modern societies.
Aims of the paper (scientific and/or social): The quality of the information received greatly influences our decisions and the procedures that follows, but equally presents a security challenge in the context of disinformation and the influence of various actors in democratic and security processes.
Methodology/Design: Technological advances have encouraged, both qualitatively and quantitatively, the development of media and other information providers from which citizens acquire diverse knowledge and receive numerous and meaningful information with the opportunity to further process and distribute it, but also to make decisions of security and national importance.
Research/Paper limitation: The paper analyzed the relevant academic literature.
Results/Findings: Of the three components for considering a country's cyber security level: technology, procedures and human resources - the latter are perhaps the most challenging component for development within national security policy and doctrine.
General Conclusion: The development of media and information literacy is becoming increasingly important for national security and cyber security strategies, but also a feasible opportunity for all countries to actively and effectively work on a viable and sustainable model for raising cyber security levels and awareness.
Research/Paper Validity: With digital transformation of society and the development of new generations in the digital environment, media and information literacy are becoming increasingly important elements for considering the education system, lifelong learning, democratic societies and active citizenship, and cyber security in all countries.

Keywords

Media and Information Literacy, Information and Cyber Security, Digital Transformation of Society, National Security.

1. Digitalna transformacija društva i sigurnosti

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 autonomno razvijen i realizovan kao izraz nosioca suvereniteta u demokratskom društvu kojem je zagarantovana sigurnost (vidi: Rousseau, 1950).

Pretpostavka za razvoj društva, kao i osnov za reprodukciju, multiplikaciju i akumulaciju znanja, jest komunikacija. Komunikacija je prošla svoj dug i daleki put od pećinskog crteža do TCP/IP-a, digitalnih metapodataka i podataka, razvoja umjetne inteligencije, algoritamskih kapija i mašinskog učenja (vidi: Crawford i Joler 2018; Perkov 2017a; 2017b; 2017c).

S druge strane, imajući u vidu da je digitalna transformacija društva donijela velike izazove u informisanju i obrazovanju, pa time i u razvoju kritičkog mišljenja - osjetljivost građana (pa i cijelog društvenog sistema) na hibridne asimetrične distorzije[489] i napade (vanjske i unutrašnje) proporcijalno se povećala, te su i izazovi za sigurnost postali značajniji (vidi: Podumljak, 2018). U nekom prethodnom periodu prije Zuckerberg ere, društvo je bilo organizovano na način da su se znali *gatekeeperi*[490] koji imaju ulogu da društvo razvijaju i usmjeravaju na društeno prihvatljiv i očekivan način. U to se ubrajaju, prije svega, mediji kao čuvari demokratije (mainstream, profesionalni – kao glavni posrednici u informisanju, pa i obrazovanju, ali i zabavi), zatim obrazovni sistem i biblioteke (kao ekskluzivni tumači, vlasnici i donosioci znanja), te vojska i policija, preko kojih država upravlja jedinim legitimnim aparatom za prisilu (kao ekskluzivni alati za unutrašnju i vanjsku sigurnost, održavanje mira, ali i, po potrebi, alati za napad i odbranu).

Međutim, uslijed apomedijacije u složenom medijskom, informacijskom, obrazovnom i sigurnosnom okruženju, tradicionalni *gatekeeperi* gube svoju pretpostavljenu ili očekivanu ulogu, te većinu tereta poimanja društveno-političke zbilje, pa i sigurnosne kulture (i u tom kontekstu cyber higijene), preuzimaju na sebe sami građani. Tako se onda pojavljuju 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). Na taj se način život modernih informacijskih društva sve više integriše u cyber prostor, a samim time i sigurnosni izazovi sve više proizlaze iz 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.

U vezi s tim, u Deklaraciji o značaju medijske i informacijske pismenosti u Bosni i Hercegovini491, ističe se da: „Medijska i informacijska pismenost (MIP) jest preduslov održivog razvoja otvorenih, pluralnih, inkluzivnih i participativnih društava znanja, te

---

[489] 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. Npr. Podumljak (2018) navodi: „8. novembra 2016. Donald J. Trump osvojio je izborni koledž sa 304 glasa, u usporedbi s 227 glasova Hillary Clinton. Dok je Clinton pobijedila u glasanju naroda - 65,84 milijuna protiv 62,98 milijuna za Donalda Trumpa – Trump je taj koji je postao 45. predsjednik Sjedinjenih Država. Robert Mercer je još jednom postigao mega ***distorziju*** tržišta kao rezultat svog utjecaja na političko ponašanje. Ovaj je put osvojio još veću nagradu: s Trumpom na vlasti šansa da utječe na još mnogo političkih događaja i na mnoge igre u isto vrijeme“ (str. 35). (…) „Njegov fond zaradio je milijarde od referenduma o Brexitu i njegove prve "kontrolirane" tržišine ***distorzije“*** (str. 37).

[490] Gatekeeper: *engl.* Vratar, čuvar vrata ili ključeva; osoba ili stvar koja kontrolira pristup nečemu.

[491] Deklaracija dostupna na:
https://www.onlinepeticija.com/deklaracija_o_znaaju_medijske_i_informacijske_pismenosti_u_BiH
i na: http://fpn.unsa.ba/b/medijska-i-informacijska-pismenost/

građanskih institucija, organizacija, zajednica i pojedinaca koji čine ta društva.". Navedena se postavka u Deklaraciji nudi i kao šira, preciznija definicija:

„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" (Deklaracija 2019).

Važno je, međutim, podcrtati da razvojem tehnike i tehnologije, cyber prostora i novih informacijskih i medijskih kanala, alata i platformi, te ulaskom u informacijsko društvo u digitalnom okruženju - sigurnosne prijetnje i izazovi izlaze iz okvira tradicionalnog poimanja međunarodnopravno definisanog i razumijevanog koncepta ratova (sukoba, konflikta), te ulazi u sferu hibridnih asimetričnih sigurnosnih izazova i ratova (Schmitt, 2017).

Pri tome, svakako, valja imati u vidu i da je „znanstveno-tehnološka racionalnost postindustrijske ere utkana u neprozirnu infrastrukturu mašinski upravljane društvenosti", te da je ta, „samokolonizacija neuromedijima" (Hibert 2018: 17) distribuirana kroz pametne uređaje građana koji su, praktično, u isto vrijeme: korisnici usluga i sadržaja, proizvođači sadržaja i metapodataka, pa i sam proizvod u situaciji i vremenu kad je informacija (tj. podatak/data) postala vrednija od nafte (Economist, 2017). Ta je okolnost ne samo „izmijenila način organizacije naših života već je i postala prepreka kognitivnoj autonomiji" (Lynch, 2016 u Hibert, 2018). Tako su građani, zapravo, postali ključni element, ali i najslabija karika u sektoru sigurnosti i, prirodno, jedno od mogućih doluznih oruđa ili očiglednih meta napada. Ipak, „informacijsko-komunikacijske tehnologije nisu puki alati već sile novog ekosistema koje utječu na našu percepciju sebe, interakcije i međusobne odnose, kao i predstavu stvarnosti" (Floridi, 2014 u Hibert, 2018), ali su oni i novi kanali pristupa do građana kojim se mogu kreirati distorzije stvarnosti, javnog mnijenja, volje, pa i manipulacije i stimulacije za djelovanje. Shodno tome, možemo pretpostaviti da se na sve to može odgovoriti jedino adekvatnim sistemskim, dugoročnim, izvodljivim i održivim pristupom medijskoj i informacijskoj pismenosti, jer je očigledno da su ostali demokratski mehanizmi već „hakirani" (vidi: Amer, 2019).

Medijska i informacijska pismenost je krovna kompetencija za: definisanje i artikulaciju informacijskih potreba; lociranje i pristup informacijama; procjenu informacija; organizovanje informacija; etično korištenje informacija; prenošenje informacija; korišćenje vještina IKT za obradu informacija; poznavanje uloge i funkcija medija u

demokratskim društvima; shvatanje uslova pod kojima mediji mogu vršiti svoje funkcije; kritičko vrednovanje medijskih sadržaja, s obzirom na predviđene funkcije medija; korištenje medija za samoizražavanje i demokratsko učešće; vještine prikazivanja (uključujući IKT), potrebne za kreiranje korisničkih sadržaja (Wilson i sar., 2015: 18; Grizzle, A. i Torras Calvo, M., 2013).

Sve su navedene kompetencije važne, građaninu potrebne da ga osnaže kako bi se nosio sa novom ulogom gatekeepera u digitalnom okruženju, pa i ključnog elementa cyber sigurnosti – individualne, institucionalne, državne, ali i međunarodne, jer sam „status tehnološke akceleracije, koji nerijetko ostaje izvan domašaja razumijevanja i kontrole netizena (Hauben i Hauben, 1997 u Hibert, 2018), dodatno pogoduje ambijentu internalizacije digitalnog zagađenja“ (dezinformacije, manipulacije, itd.) „amplificiranog algoritamskim upravljanjem i reorganiziranjem ljudskog kapitala (pažnje, podataka i privatnosti).“ (Hibert, 2018: 19).

U konačnici, pred građaninom, ali i društvom, državom i sektorom sigurnosti - postavljeni su izazovi za koje uglavnom nije dorastao (vidi: Bartlett 2018; Rees 2018; Bostrom 2014) i to, prije svega, zbog neadekvatnog sistemskog odgovora obrazovnog i sigurnosnog sektora na digitalnu transformaciju, u ovom kontekstu u segmentu cyber sigurnosti.

2. Strategije cyber sigurnosti

Sama digitalna transformacija društva učinila je velike pomake u razvoju nauke i tehnologije, kao i u procesima učenja i komunikacije, ali i doprinijela da čitavo sigurnosno poimanje svakodnevnice, pa i njezino izučavanje ili razumijevanje, postane značajno kompleksnije. Prenošenjem većine društvenih, ekonomskih i političkih sfera u cyber prostor, i sigurnost biva izložena novim izazovima, rizicima, pojavnim oblicima, što neminovno zahtijeva i prilagođene strateške, operativne i taktičke sigurnosne odgovore.

Neizbježan razvoj cyber-sigurnosne nauke, kao primijenjene i interdisciplinarne djelatnosti, razvija holistički pristup razumijevanju novih okolnosti i izazova u digitalnom okruženju, dakle pristup koji ima svoje poveznice sa onima iz analognog svijeta u razumijevanju, razvoju i praksi cyber sigurnosti (vidi: Dykstra 2016: 1-15).

Termin „cyber sigurnost“ treba u datom terminosistemu razumijevati kao složen pojam koji ove dvije riječi spaja u navedenu sintagmu: Cyber se odnosi na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, a posebno Internetom i informacijskim tehnologijama (OSCE 2019), dok termin Sigurnost ima korijene u starolatinskom izrazu securus (bezbrižan, pouzdan, siguran; Klaić, 1985 u Beridan, 2007) što u „znanosti, i u političkoj praksi (...) podrazumijeva dva svoja osnovna aspekta: – znači istodobno: a) funkciju, djelatnost države, društva i pojedinca, a potom i b) stanje u odnosima među državama, stanje unutar jedne države, među ljudima, odnosno stanje u prirodi i kosmosu spram života općenito“ (Beridan 2007: 100).

Na osnovu Beridanove izvedbe definicije sigurnosti (2007: 101), može se reći da sigurnost „općenito podrazumijeva stepen zaštićenosti ljudi od različitih oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države“ i međunarodnih odnosa, pa i na kosmičkom i planetarnom nivou života općenito, ljudskoga roda u cjelini „od svih vidova ugrožavanja“. Sigurnost podrazumijeva stepen zaštićenosti od ugrožavanja, uz naglasak da ne postoji apsolutna i potpuna sigurnost, već možemo govoriti o većem ili manjem stepenu sigurnosti.

U tom kontekstu moguće je zaključiti da 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, radi jednostavnijeg razumijevanja, prije svega potrebno posmatrati kao cilj ili kao sredstvo (1) u cyber kriminalitetu, (2) u politički motivisanim cyber napadima i (3) u cyber terorizmu.

1. Cyber kriminalitet uključuje pojedince ili grupe koji „ciljaju“ IKT sisteme za finansijsku protupravnu dobit ili za pravljenje (društvene, ekonomske, političke, sigurnosne) disrupcije. Ovdje govorimo o obliku kriminalnog ponašanja kod kojega se korištenje IK tehnologije i sistema upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka krivično-pravno relevantna posljedica. Kompjuterski kriminalitet je, također, protivpravna povreda imovine kod koje se računarski podaci s predumišljajem mijenjaju (manipulacija računara), razaraju (računarska sabotaža) ili se koriste zajedno s hardverom (krađa).492

2. Cyber napadi često uključuju politički motivisano prikupljanje informacija i/ili onesposobljavanje ključne / kritične infrastrukture, pa čak i stvaranje distorzija u društveno-političkom životu zajednice. Sve češće su prikriveni vidovi specijalnog informacijskog ratovanja koji su teško prepoznatljivi u dinamično digitalnom medijskom okruženju. Razvoj moći i kapaciteta visokotehnoloških kompanija, prikupljanje podataka i metapodataka, te njihova dostupnost onome ko je spreman platiti - razvija i nove modele specijalnog asimetričnog hibridnog informacijskog ratovanja, koji uključuju i pomoć algoritamski determinisanih društvenih mreža, dezinformacijsko-propagandne kampanje i intimno poznavanje individualnih građana na osnovu akumuliranih podataka (data points) i digitalnog traga. (vidi: Crawford i Joler 2018; Perkov 2017a; 2017b; 2017c)

[492] Vidi: Krivični zakon Federacije Bosne i Hercegovine "Službene novine Federacije BiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017: gl. XXXII

3. Cyber terorizam ima za cilj da smišljenom upotrebom napada (ili prijetnje) na IKT sisteme izazove strah, te da se, s namjerom prisiljavanja ili zastrašivanja vlasti ili društva, postignu ciljevi koji su općenito politički, vjerski ili ideološki. Uz to, teroristi i terorističke organizacije jednako efikasno koriste cyber prostor za propagandu, regrutovanje novih kadrova, kao i komunikaciju sa javnostima i medijima (vidi: Babić, 2015).

Načelno, cyber sigurnost gledamo sa aspekta sposobnosti države da odgovori na prijetnje, incidente, i organizuje adekvatnu otpornost sigurnosnog sistema i elemente: snage, mjere, funkcije i aktivnosti sistema nacionalne sigurnosti (vidi: Beridan 2007).

U tu svrhu se izrađuju državne strategije cyber sigurnosti. U okruženju cyber prijetnji (koje je promjenljiva kategorija), države moraju imati fleksibilne i dinamične strategije cyber sigurnosti. Državna strategija za cyber sigurnost jest plan mjera namijenjen poboljšanju sigurnosti i otpornosti infrastruktura i usluga; njome se određuje niz nacionalnih ciljeva i prioriteta koji bi se trebali postići u određenom vremenskom okviru.

Osim rješavanja izazova cyber sigurnosti, strategije se temelje na saradnji – unutrašnjoj i vanjskoj ili međunarodnoj. Neke od najvažnijih postavki za poboljšanje saradnje između sudionika jesu razmjena informacija i stvaranje javno-privatnog partnerstva.493 S obzirom na okruženje rizika i prijetnji koje mutiraju, razvijaju se, konvergiraju i mimikriraju, sigurnost u stanju statičnosti nije adekvatno rješenje u cyber okruženju. Cyber sigurnost je proces (pa čak se može reći i životna filozofija, stanje uma) koji se odnosi na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, posebno sa internetom i informacionim tehnologijama. U tom kontekstu cyber prostor je više nego internet, jer „uključuje ne samo hardver, softver i informacione sisteme, već i ljude i društvenu interakciju u okviru ovih mreža“ (OSCE 2019: 34).

Tri ključna elementa cyber sigurnosti, potrebna za sveobuhvato poimanje, jesu: tehnologija, procedure i ljudski resursi.

U pogledu tehnologije, koliko god se taj aspekt cyber sigurnosti na prvi pogled činio kompleksnim, u većini slučajeva postoje (polu)gotova hardwerska i softwerska rješenja koja se kupuju od specijaliziranih kompanija (vidi: Microsoft, Cisco, itd). Samo manji broj država ima kapacitete da razvijaju vlastitu tehnologiju, hardware, software, alate, pa i cyber oružja. Tako, naprimjer, Sjedinjene Američke Države kao vodeća država po ulaganju u sigurnost i oružane snage, kontinuirano i sve više ulažu u cyber sigurnost, pa je tako trenutno (za 2020.) za federalne institucije iz budžeta planirano 17,5 milijardi USD, odnosno, ukupno je procijenjenih 66 milijardi USD koje se u SAD ulažu u cyber sigurnost (Forrest 2016; The White House, 2019; Statista, 2019).

---

493 Više na: The European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/

Drugi element cyber sigurnosti jesu procedure, uglavnom zasnovane na konceptima sistema informacijske sigurnosti (npr. ISO/IEC 27000 grupa standarda), a one jasno propisuju da kroz uspostavljanje i upravljanje tim sistemom, javna uprava (ali i komercijalni sektor, i sami građani) dosljedno izvršava svoju ulogu u izgradnji informacionog društva (vidi: Calder i Watkins, 2015).

Menadžment informacijske sigurnosti posebno je bitan za javne institucije, što znači da „razvojem sistema informacijske sigurnosti javna uprava uspostavlja preventivne mjere i stvara organizaciono-tehničke preduvjete za sistemski razvoj zaštitnih i represivnih mjera u okviru informacijskog društva. Ti procesi ne mogu se uspješno sprovoditi bez uspostavljanja konzistentnog sistema informacijske sigurnosti (…) Pod politikom upravljanja informacijske sigurnosti podrazumijeva se hijerarhijski uređen skup dokumenta koji predstavlja osnovu za implementaciju sistema upravljanja informacijske sigurnosti.“494

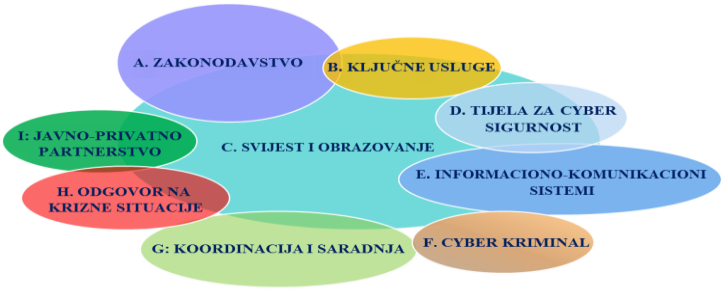
Na kraju, ljudski resursi koji su možda i najvažniji segment ekosistema cyber sigurnosti. Ljudske resurse treba posmatrati dvojako: 1) kao relativno mali broj visoko kvalifikovanih stručnjaka (uglavnom u oblasti IKT), te 2) kao širu grupu ostalih uposlenika, ali i ukupno građanstvo kao aktivne ili pasivne sudionike u cyber prostoru. Prvi su stručnjaci koji su završili obrazovanje za rad u cybersigurnosnom okruženju i koji su toliko traženi da ih je sve teže zadržati na radu u državnom / javnom sektoru. Za druge je (praktično sve ostale građane) prije svega potreban skup kompetencija koje se mogu objediniti pod konceptom medijske i informacijske pismenosti. Izostanak takvih kompetencija proporcionalno povećava sigunosni rizik, jer građanin, zaposlenik u firmi koji ima pristup mreži, javni službenik, pa i agent sigurnosnih službi bez medijske i informacijske pismenosti nedvojbeno jest najslabija karika u cyber sigurnosti. Najčešće cyber napadi ciljaju upravo najslabije tačke (Symantec, 2019), tj. ljude koji su sigurnosno interesantni i nedovoljno medijski i informacijski pismeni.

Medijska i informacijska pismenost zauzima značaj segment obrazovanja i pismenosti današnjice (Vajzović 2017; Vajzović i sar., 2018; Vajzović i sar., 2019). Kompetencije ljudi u segmentu građanske pismenosti postale su ključne u vremenu kada je, zbog postepenog gubljenja sistemske uloge gatekeepera, teret donošenja odluka više nego ikada na pojedincima. Tradicionalni mediji, obrazovni sistem, sigurnosni sistem, pa i porodica, sve više i sve očitije gube bitku u dominaciji naspram interneta i cyber okruženja.

[494] Vidi: Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine. Službeni glasnik Bosne i Hercegovine br. 2017/38

U pogledu holističkog sagledavanja izazova, jasno definisani strateški ciljevi cyber sigurnosti pomažu cjelokupnom društvu da razvije adekvatnu cyber sigurnost, kao što je izloženo u grafikonu 1.

Grafikon 1. *Strateški ciljevi cyber sigurnosti*



Izvor: Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini (2019).[495]

Iz grafikona 1. jasno je vidljivo da je razvijanje svijesti o cyber sigurnosti i obrazovanje u toj oblasti značajan i povezujući element za sve ostalo, što se navodi u cilju C (Podizanje nivoa svijesti i znanja o cyber sigurnosti i podciljevima), C1 (Podizanje svijesti o cyber sigurnosti) i C2 (Jačanje programa treninga i obrazovanja). Iz tih je razloga posebno važno „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).

3. Osnaživanje građana kroz MIP kao strateško opredjeljenje cyber sigurnosti

Cyber sigurnost je izazov za međunarodno (humanitarno) pravo, međunarodne organizacije, multinacionalne korporacije i pojedinačne države, za društvo i za pojedinca. Iz te okolnosti proizlazi da je koncept cyber sigurnosti i značaj osnaživanja te vrste sigurnosnih pitanja kroz medijsku i informacijsku pismenost važno i nužno razumijevati i

[495] Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini je dokument koji je izradila neformalne radna grupa stručnjaka iz javnih, privatnih i akademskih institucija, pod okriljem Misije OSCE-a u Bosni i Hercegovini, a na poziv Ministarstva sigurnosti Bosne i Hercegovine.

pratiti na tri osnovna nivoa: individualnom, institucionalnom, te državnom i međunarodnom nivou.

1. Individualni nivo – gdje je značajna cyber sigurnosna higijena, ali i suštinsko razumijevanje informacija, sadržaja i medija u digitalnom okruženju, kao i shvatanje kompleksnosti infrastrukture i arhitekture dezinformacija i moći ubjeđivanja građana koji nisu medijski i informacijski mudri i osnaženi (vidi: Car, 2015). Praktično to znači da više ne govorimo samo o Clickbaitu[496] i farmama portala ili naloga na društvenim mrežama za potrebe pribavljanja imovinske koristi[497], već govorimo o smjenama vlada, izborima izvršne i zakonodavne vlasti, promjeni ustava, okupacijama ili strateškim ubjeđenjima širokih narodnih masa, pa i podrški za „konvencionalno" ratovanje – šta god to danas značilo u doba dronova, autonomnih oružanih sistema, umjetne inteligencije u i slično (vidi: Giles, 2016).

2. Institucionalni nivo – gdje upravljanje sistemima informacijske sigurnosti, sa bazom u medijskoj i informacijskoj pismenosti na nivou organizacijskih jedinica / kompanija, postaje ključan element sigurnosti kolektiva (vidi: Armerding, 2018).

3. Državni i međunarodni nivo – gdje je fokus na saradnji i izgradnji povjerenja, a medijska i informacijska pismenost značajna, kao strateško opredjeljenje, za podizanje digitalne sigurnosne kulture, za obrazovanje i podizanje svijesti, te za jačanje otpornosti cijelog društva na hibridne asimetrične napade i distorzije u demokratskim društvima.

Brojni su primjeri narušavanja cyber sigurnosti, distorzije društveno-političkog sistema i hibridnih asimetričnih napada koji se odnose na sva tri nivoa, kao što su, primjerice:

1. Estonija[498] - Od 27. aprila 2007. svakodnevnicu u Estoniju čine cyber-napadi, informacijsko ratovanje, lažne vijesti. Te 2007. godine su je pogodili i cyber-napadi velikog obima koji su u nekim slučajevima trajali sedmicama. Internetske usluge estonskih banaka, medijskih kuća i državnih tijela su srušeni sa neviđenim nivom internetskog prometa. Uzastopni valovi napada spamovima od botnete i ogromne količine automatiziranih internetskih zahtjeva preplavile su servere. Rezultat je za građane Estonije bio da su bankomati i internetske bankarske usluge bile sporadično van funkcije; Vladini zaposlenici nisu bili u mogućnosti komunicirati jedni s drugima putem e-pošte; a novine i televizijske stanice iznenada su otkrile da ne mogu isporučiti vijesti.
2. Ukrajina (Brantly, Cal i Winkelstein: 2017) - Otkako su političke krize započele 2014. godine, u Ukrajini je više nego u bilo kojem drugom sukobu, uključivale širok spektar metoda: konvencionalnu taktiku, cyber operacije, elektroničko

[496] Engl. Clickbait - izraz kojim se opisuju senzacionalistički naslovi članaka koji čitateljima web portala navodno nude ekskluzivan ili nesvakidašnji sadržaj. Izraz je složenica engleskih riječi *click* (klik) i *bait* (mamac).
[497] Više na: https://raskrinkavanje.ba/analiza/farme-portala-sarajevo-grad
[498] Vidi: https://www.bbc.com/news/39655415

ratovanje i informacijsko ratovanje. Kombinirani izazovi neprekidnog sukoba, nejasnih boraca i raznolike primjene fizičke, informacijske, elektroničke i cyber sile prema zvaničnim ukrajinskim snagama duž crte razgraničenja, ali i ukrajinskim građanima širom zemlje predstavljaju novu upotrebu moći radi postizanja političkih ciljeva. Tu se ističu i cyber napad na elektroenergetsku mrežu u decembru 2015. godine i niz snažnih cyber napada s zlonamjernim softverom Petya iz 2017. godine.

3. Gruzija (Cornell i Starr, 2009) - U augustu 2008. Rusija je optužena da je koristila cyber uz oružane napade protiv Gruzije: napad na vladine web resurse sa ciljem nanošenja štete ugledu; ugašeni su mediji, forumi i blogovi u Gruziji sa rezultatom da ljudi nisu mogli dobiti prave informacije, uz istovremeno dezinformacije o stvarnim činjenicama od strane ruskih medija; blokirani i prekinuti su gruzijski internetski resursi: Internet komunikacija je bila nemoguća u zemlji i van nje.
4. Cambridge Analitika sa projektima Brexit i Trump499 (Podumljak, 2018; Amer, 2019) - Tvrtka za analizu podataka koja je radila s izbornim timom Donalda Trumpa i pobjedničkom kampanjom Brexit sakupila je milijune Facebook profila birača, u jednom od najvećih tehnoloških kršenja ikada, i koristila ih za izgradnju moćnog softverskog programa za predviđanje i utjecaj na izbore. Steve Bannon 2014. godine - tada izvršni predsjedavajući „ultra desničarske" informativne mreže Breitbart i Robert Mercer, američki milijarder hedge fondova i republikanski donator, bili su kreatori i investitori u Cambridge Analitika. Njihova ideja je bila da spoje „big data" i društvene mreže/medije u poznate vojne metodologije - „informacijskih operacija" - a zatim je iskoriste za američke izbore.

Činjenica da se o hibridnim napadima u novije vrijeme sve češće razmišlja i sve više govori, potvrđuju i riječi ljudi „od struke". Tako generalpukovnik Senad Mašović, načelnik Zajedničkog štaba Oružanih snaga BiH upozorava na nužnost da „kao država prepoznamo module hibridnog rata. Iako ne postoji dogovorena definicija hibridnog ratovanja», smatra da „za ono što je uobičajeno u posljednjih desetak godina, ta djelovanja možemo prepoznati i na našim prostorima", te podsjeća „da su asimetrične prijetnje stalno prisutne, da imaju za cilj sprječavanje funkcionisanja državnih institucija, stvaranje političke i ekonomske nesigurnosti, stvaranje negativnog mišljenja i nezadovoljstva kod stanovništva, kao i nepovoljnih ekonomskih prilika. Posebno je ova problematika izražena u stvaranju negativne slike koja dovodi do masovnog odlaska mladih ljudi koji ne vide perspektivu u svojoj državi, što se dalje negativno odražava na cjelokupno stanje" (Čavčić 2019).

Za državu je i za cyber sigurnost postojanje dobro organizovanih CERT / CSIRT500 ključno u smislu adekvatnih odgovora na incidente i prijetnje, kao i u pogledu njihove aktivne

[499] Za više informcija, dostupno na: https://www.theguardian.com/news/series/cambridge-analytica-files
[500] CSIRT (Computer Security Incident Response Team) - tim za odgovor na računarske sigurnosne incidente

uloge u saradnji sa drugim državama i međunarodnim organizacijama. Njihova saradnja na platformama poput FIRST-a501 kao međunarodnog foruma timova za odgovor na računarske sigurnosne incidente, posebno je značajna za globalnu sigurnost. Okupljajući timove osposobljene za odgovore na različita pitanja i izazove računalne sigurnosti iz vladinih, poslovnih i obrazovnih organizacija, FIRST promovira suradnju i koordinaciju u prevenciji incidenata, inicira brzu reakciju na incidente i podržava razmjenu informacija među članovima i zajednicom u cjelini.

4. Zaključni osvrt

Vidjeli smo da je digitalna transformacija društva donijela velike izazove u informisanju i obrazovanju, pa time i u razvoju kritičkog mišljenja. Život modernih informacijskih društva sve više integriše u cyber prostor, a samim time i sigurnosni izazovi sve više proizlaze iz istog domena. 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. Kako smo naveli, uslijed apomedijacije u složenom medijskom, informacijskom, obrazovnom i sigurnosnom okruženju, tradicionalni gatekeeperi gube svoju pretpostavljenu ili očekivanu ulogu, te većinu tereta poimanja društveno-političke zbilje, pa i sigurnosne kulture (i u tom kontekstu cyber higijene), preuzimaju na sebe sami građani. Iz svega je vrlo jasno zašto se (za 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.

Na kraju je, umjesto zaključka, važno još jedanput ukratko potcrtati da bi kao temelj daljnjeg razvoja i podizanja nivoa cyber sigurnosti, trebalo biti podizanje nivoa medijske i informacijske pismenosti, kao strateškog opredjeljenja opšteg razvoja cyber-sigurnosnog domena, te usavršavanja otpornosti na hibridne asimetrične specijalne informacijske napade i ratovanja. Na taj bi se način dugoročno i značajno osnažila nacionalna sigurnost i istovremeno olakšao posao sigurnosnim snagama u suočavanju sa novim dinamičnim izazovima cyber sigurnosti. Na individualnom planu, stvarali bi se uvjeti da građanin prestane učiti na vlastitim greškama koje nerijetko preskupo koštaju i njega samoga, ponekad i zajednicu u kojoj živi i radi.

Kako je navedeno, okruženje rizika i prijetnji mutira, razvijaja se, konvergira i mimikrira, te sigurnost u stanju statičnosti nije adekvatno rješenje u cyber okruženju. Cyber sigurnost je proces koji se odnosi na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, posebno sa internetom i informacionim tehnologijama i sadrži navedena tri ključna elementa cyber sigurnosti, potrebna za sveobuhvato poimanje: tehnologija, procedure i ljudski resursi. S obzirom da je ljudski

[501] Vidi na: www.first.org

faktor često i najslabija karika, medijska i informacijska pismenost je zasigurno možda i najznačajni segment u sistemu cyber sigurnosti.

Bibliografija:

1. Amer, K., Noujaim, J. & Amer, K., Barnett, E., Kos, P. (2019) The Great Hack. SAD
2. Armerding, T. (20.12.2018.). The 18 biggest data breaches of the 21st century. Dostupno: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
3. Babić, V. (2015) Cyber terorizam – suvremena sigurnosna prijetnja. Novi Travnik
4. Bartlett, J. (2018). The People vs Tech: How the internet is killing democracy (and how we save it). London. Ebury Press.
5. Beridan, I (2007) Politika i sigurnost – sadržaj i obilježja pojmova. Godišnjak 2007 Fakultet političkih nauka Sarajevo.
6. Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford. Oxford University Press
7. Brantly, A. F., Cal, N. M., i Winkelstein, D. P. (2017) Defending The Borderland: Ukrainian Military Experiences with IO, Cyber, and EW. The Army Cyber Institute at West Point
8. Calder, A., & Watkins, S. (2015). IT governance: an international guide to data security and ISO 27001/ISO 27002. KoganPage.
9. Car V., ur. (2015). Medijska pismenost - preduvjet za odgovorne medije. Zbornik radova sa 5. regionalne znanstvene konferencije "Vjerodostojnost medija", Sarajevo: Fakultet političkih nauka
10. 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
11. Čavčić, I. (19.11.2019.) „General Senad Mašović: Asimetrične prijetnje su stalno prisutne, Oružane snage ih znaju prepoznati“. Klix.ba. Dostupno na: https://www.klix.ba/vijesti/bih/general-senad-masovic-asimetricne-prijetnje-su-stalno-prisutne-oruzane-snage-ih-znaju-prepoznati/191119015
12. Deklaracija o značaju medijske i informacijske pismenosti u Bosni i Hercegovini, Sarajevo, 28.1.2019. dostupna na: http://fpn.unsa.ba/b/wp-content/uploads/2019/06/Deklaracija-o-znacaju-MIP-u-BiH_final_310119.pdf
13. Dykstra, J. (2016). Essential cybersecurity science: build, test, and evaluate secure systems. OReilly.
14. 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.
15. Farme portala: "Sarajevo grad". (n.d.). Dostupno na: https://raskrinkavanje.ba/analiza/farme-portala-sarajevo-grad.
16. Forrest, Conner „Obama seeks $19B for cybersecurity in 2017, a 36% increase“. TechRepublic. Objavljeno 9 Februar, 2016. dostupno na: https://www.techrepublic.com/article/obama-seeks-19b-for-cybersecurity-in-2017-a-36-increase/

17. Giles, K. (2016). Handbook of Russian information warfare. Rome, Italy: NATO Defence College Research Division.
18. Grizzle, A., Torras Calvo, M. (2013) Media and Information Literacy Policy and Strategy Guidelines. United Nations Educational
19. 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:
20. http://lida.ffos.hr/2018/datoteke/abstracts_2018/LIDA_2018_Kulenovic_paper_68.docx
21. Krivični zakon Federacije Bosne i Hercegovine "Službene novine Federacije BiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017: gl. XXXII
22. 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/
23. 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
24. Perkov, B. (01.08.2017.). Političko-informaciono ratovanje: kratko uputstvo. Dostupno: https://labs.rs/sr/politicko-informaciono-ratovanje-kratko-uputstvo/.
25. Perkov, B. (04.08.2017). Nematerijalni rad i prikupljanje podataka. Dostupno: https://labs.rs/sr/nematerijalni-rad-i-prikupljanje-podataka/.
26. Perkov, B. (17.08.2017.). Istraživanje metapodataka: Haking Tim. Dostupno: https://labs.rs/sr/istrazivanje-metapodataka-haking-tim/.
27. Podumljak, M. (2018) TRUMP'S CODE: Making Money on Populist Disorder. Partnership for Social Development (PSD), Zagreb. ISBN: 978-953-55446-6-1
28. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine. Službeni glasnik Bosne i Hercegovine br. 2017/38)
29. Rees, M. (2018) On the Future Prospects for Humanity. Princeton & Oxford. Princeton University Press
30. Rousseau, J.-J. (1950) The Social Contract and Discourses. trans. G. D. H. Cole. New York: E. P. Dutton. Pristupion na: http://www.questia.com/read/4795085/the-social-contract-and-discourses.
31. Schmitt, M. N. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
32. Statista (2019) Spending on cybersecurity in the United States from 2010 to 2018. dostupno na: https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/
33. Symantec (2019) ISTR. Dostupno na: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

34. 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
35. The European Union Agency for Cybersecurity (ENISA). Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies?tab=details
36. The Guardian. The Cambridge Analytica Files. Dostupno na: https://www.theguardian.com/news/series/cambridge-analytica-files
37. The White House. 2019. "Cybersecurity Funding". dostupno na: https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf
38. Vajzović E., Džihana A., Hibert M., Ibrahimbegović-Tihak V., Bakić S., Kulenović F. (2018). Pregledna studija o politikama i strategijama medijske i informacijske pismenosti u Bosni i Hercegovini. Sarajevo: Fakultet političkih nauka.
39. 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.
40. Vajzović, E., Turčilo, L., Cerić, H., Osmić, A., Silajdžić, L. (2019) Uvođenje medijske i informacijske pismenosti u obrazovni sistem – procjena kompetencija nastavnika za podučavanje medijske i informacijske pismenosti u Kantonu Sarajevo. Sarajevski žurnal za društvena pitanja. Godište VIII. Broj 1-2. 2019. str.137-172. Fakultet političkih nauka Univerzitet u Sarajevu
41. Wilson, C., Grizzle, A., Tuazon, R., Akyempong, K., Cheung, C.K.. (2015) Medijska i informaciona pismenost: Program obuke nastavnika. Nacionalna biblioteka Crne Gore "Đurđe Crnojević".