ORIGINALNI NAUČNI RAD

Primljeno: 13. XI 2025.
Prihvaćeno za objavljivanje: 16. I 2026.

MEDIJI I SAJBER BEZBEDNOST: PREDSTAVLJANJE SAJBER KRIMINALITETA U SRPSKOM DIGITALNOM PROSTORU[1]

Aleksandar Bogićević[2]
Institut za strategijska istraživanja, Beograd
ORCID 0009-0006-7450-5193

DOI: 10.5937/cm20-62771

Sažetak: *Oslanjajući se na primenu teorije uokviravanja, izvršena je analiza sadržaja 222 novinska članka objavljena u periodu od februara 2022. do februara 2025. godine na tri interenet portala: Radio televizije Srbije – RTS (nacionalnom javnom servisu), Kuriru (tabloidnom mediju) i Danasu (kritički orijentisanom mediju). Vesti na portalima kodirane su prema tematskom fokusu, geografskom obuhvatu, izvorima informacija, prisustvu edukativnog sadržaja i dominantnim medijskim okvirima. Cilj rada jeste ispitivanje na koji način posmatrani srpski mediji konstruišu predstave o sajber kriminalitetu i u kojoj meri ove predstave mogu doprineti edukaciji ili pak dezinformaciji javnosti u pogledu ove važne teme. Rezultati istraživanja ukazuju na to da medijsko predstavljanje sajber kriminaliteta dominantno funkcioniše kroz okvir konflikta i pripisivanja odgovornosti sa posebnim naglaskom na međudržavne sajber napade u kontekstu sukoba u Ukrajini. Sa druge strane, percepcija sajber incidenata koji su se dogodili na teritoriji Srbije u velikoj meri je uslovljena uredničkom orijentacijom i vrednosnim odnosom posmatranog medija prema aktuelnoj političkoj vlasti. Važno je istaći da, iako je prisutan sadržaj koji se može oceniti kao edukativan i usmeren na podizanje svesti pojedinaca o sajber bezbednosti, on je često potisnut senzacionalističkim i pojednostavljenim izveštavanjem. Rad zaključuje da posmatrani mediji, uprkos tome što prepoznaju rastući značaj sajber pretnji, još uvek nisu u potpunosti prilagodili svoje izveštavanje složenostima sajber kriminaliteta. Preferiranje senzacionalizma i*

[1] Rad je nastao kao deo projekta Ministarstva odbrane: „Bezbednosni izazovi zemalja Zapadnog Balkana u evropskoj bezbednosnoj paradigmi", br. ISI/DH1/24-25, a koji istraživački tim i istraživačka grupa za proučavanje regionalne bezbednosti Instituta za strategijska istraživanja i spoljnih saradnika realizuje u periodu 2024-2025.

[2] Kontakt sa autorom: aleksandarbogicevic32@gmail.com

institucionalnih narativa umesto kritičkog pristupa može dovesti do iskrivljene percepcije javnosti o sajber bezbednosti. Ipak, identifikovano prisustvo poruka o prevenciji i edukaciji ukazuje na potencijal medija kao važne komponente društvene otpornosti u digitalnom dobu.

Ključne reči: *sajber kriminal, medijski diskurs, sajber bezbednost, Srbija, društvena otpornost*

1. Uvod

Digitalizacija svakodnevnog života u modernom društvu uticala je na pojavu novih vrsta rizika i pretnji koje obuhvata i prenošenje kriminaliteta iz fizičkog prostora u virtuelni, stvarajući time potpuno novu dimenziju za sprovođenje ilegalnih aktivnosti. Jednostavno prevazilaženje strogo regulisanih državnih granica i prevazilaženje prostorne distance, koji su olakšani upotrebom savremenih tehnologija, pružili su kriminalcima nove mogućnosti, kako u pogledu različitih oblika nelegalnih aktivnosti, tako i u pogledu raznovrsnosti potencijalnih žrtava. Određeni stepen anonimnosti koji karakteriše sajber prostor, u kombinaciji sa ograničenom sposobnošću država da privedu pravdi učinioce usled ograničene primene principa univerzalne jurisdikcije i prisustva prekograničnih pravnih ograničenja, doprinose stvaranju atmosfere nedodirljivosti i percepcije nekažnjivosti među izvršiocima ove vrste krivičnih dela (Wall, 2007). U okruženju u kome sajber kriminalci pravazilaze „barijere geografije" (Dhasmana et al, 2024: 210) izbegavajući time kažnjavanje, pojedinci se okreću sopstvenim kapacitetima i znanjima kako bi sprečili da postanu žrtve sajber kriminala. Pitanje informacione bezbednosti, nekada rezervisano za usku ekspertsku zajednicu, danas obuhvata znatno veću grupu zainteresovanih društvenih aktera: donosioce političkih odluka, medije, privredu, građane, nevladine organizacije i međunarodne institucije (Boholm, 2021: 2).

Spuštanje odbrane od sajber kriminaliteta na individualni nivo zahteva od pojedinaca najčešće samostalnu edukaciju o rizicima i pretnjama u čemu su internet portali specijalizovani za pružanje saveta u pogledu održavanja „sajber higijene" prepoznati kao jedan od glavnih mehanizama u prevenciji sajber kriminala (Skopik, Settanni & Fiedler, 2016). Međutim, pažnja građana je znatno više usmerena prema etabliranim medijima kao izvoru informacija zbog čega oni imaju veoma važnu ulogu u diseminaciji znanja (Mazrouei, Čigoja Piper, & Connolly, 2022: 2; Happer, & Philo, 2013: 321; Ilić, 2017: 37). Njihova spo-

sobnost da istaknu u prvi plan društvene pojave i probleme može predstavljati efikasan instrument podizanja društvene svesti o rizicima koje nosi nesmotreno ponašanje u sajber prostoru. Sa druge strane, slika koju mediji pružaju javnosti o sajber kriminalitetu karakterišu senzacionalizam i uprošćavanja (Abdugoffo-rov, 2024: 2; Greer, 2013: 31) čime kreirani narativi mogu štetiti percepciji problema od strane javnosti. Fokus na vestima koje se bave napadima na značajne mete kao što su državne institucije i multinacionalne kompanije dodatno skreće pažnju sa najranjivije kategorije korisnika interneta – običnih građana.

Kako su etablirane medijske kuće glavni izvori informacija javnosti u pogledu kriminaliteta, a posebno onog koji se odvija izvan neposrednog iskustva čitaoca (Gomes, Sardá, & Granja, 2022: 9), što je naročito izraženo u slučaju sajber kriminaliteta, javlja se potreba za detaljnijom analizom postojećih medijskih narativa. Takva analiza je ključna kako bi se razumela priroda poruka koje se diseminiraju u javnosti. Imajući u vidu da većina građana nikada nije imala neposredan susret sa sajber kriminalitetom, uloga medija kao instrumenta u oblikovanju mišljenja javnosti postaje još izraženija (Rader, Wash, 2015: 121). Polazeći od ovih pretpostavki, ovaj rad nastoji da, primenom teorije uokviravanja (eng. *Framing Theory*) i fokusiranjem na dva ključna aspekta medijskog uticaja, izbor tema koje se predstavljaju javnosti i način njihove interpretacije (Buse & Meißner, 2019: 105–106), utvrdi karakteristike medijskih narativa o sajber kriminalitetu u domaćoj javnosti. Takođe, istraživanje nastoji da sagleda potencijal medija da kreiraju sadržaj koji omogućava čitaocima usvajanje novih znanja i jačanje ukupne društvene otpornosti na ovakve pretnje. Dosadašnja istraživanja na polju analize medija u Srbiji bila su usmerena na ključne političke događaje kao što su protesti 2017. godine (Krstić, Milojević, Kleut, 2018), na prikaz diskriminisanih i osetljivih društvenim grupama (Trajković, 2020; Milutinović & Pavlović, 2019), kao i na pitanje kriminaliteta (Banović & Ilić, 2019). Međutim, jedno od polja istraživanja medijskog izveštavanja koje privlači pažnju inostranih istraživača, a koje do sada nije bilo zastupljeno u Srbiji jeste analiza izveštavanja o sajber kriminalitetu (Mazrouei, Čigoja Piper, & Connolly, 2022) kao relativno novoj pojavi koja ima rastući značaj za savremeno društvo. Ovo istraživanje doprinosi popunjavanju uočene praznine u literaturi, istovremeno omogućavajući bolje razumevanje načina na koji dominantni mediji u Srbiji oblikuju narative u kontekstu sve prisutnijeg fenomena sajber kriminala.

2. Sajber kriminalitet: pojam, oblici i društveni rizici

Brojnost pojmova kojima se može označiti sajber kriminalitet[3] praćen je jednako raznolikim pristupima njegovom definisanju, što ukazuje na teorijsku i normativnu neusaglašenost koja i dalje obeležava ovu oblast. Tako Donalds (eng. *Charlette Donalds*) i Osej-Brajson (eng. *Kweku-Muata Osei-Bryson*) pod „digitalnim kriminalom" podrazumevaju sva nezakonita dela učinjena protiv računara, uređaja povezanih sa računarom ili informaciono-tehnoloških mreža, uključujući i tradicionalne kriminalne radnje koje su usmerene protiv pojedinaca koji koriste internet ili računarsku tehnologiju. (2019: 403) Sveobuhvatnu definiciju daju i Stošić i Janković, podrazumevajući pod terminom „sajber kriminal" izvršenje krivičnih dela u kojima je računar sredstvo ili predmet krivičnog dela i u kojima su sve potencijalne žrtve nezavisne od starosti, pola i mesta stanovanja (2022: 84). Ovakva određenja sajber kriminaliteta ukazuju na vrlo širok dijapazon aktivnosti koje kriminalci mogu preduzeti kako bi naneli štetu pojedincima, organizacijama ili državama, što dodatno usložnjava nastojanja naučne i stručne javnosti da uspostave jedinstven i sveobuhvatan pojmovni okvir ove pojave.

Sajber kriminalitet odlikuje se raznovrsnošću manifestacionih oblika, što je uslovilo postojanje više pristupa klasifikaciji. Prema kategorizaciji koju su usvojile Ujedinjene nacije, sve forme sajber kriminaliteta svrstavaju se u pet osnovnih grupa: neautorizovan pristup podacima, onesposobljavanje računara i računarskih mreža, špijunaža, nanošenje štete računarima i presretanje podataka u mreži (United Nations, 2000: 3) Sa druge strane, Mekgvajer (eng. *Mike McGuire*) i Dauling (eng. *Samantha Dowling*) pristupaju klasifikaciji sajber kriminaliteta kroz dihotomiju zasnovanu na stepenu zavisnosti od informaciono-komunikacionih tehnologija koja je prisutna i u domaćem pravnom okviru (Zakonu o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, 2005). Prvu grupu predstavljaju kriminalne radnje zavisne od postojanja računara ili drugih informaciono-komunikacionih tehnologija i u njih se mogu svrstati ilegalne radnje kao što su DDOS napadi, distribucija malicioznih programa, upadi u računarske mreže ili upravljanje botnet mrežama

[3] Kao sinonimi pojmu sajber kriminala u literaturi često se koriste i pojmovi kao što su *digitalni kriminal*, *internet kriminal* ili *visokotehnološki kriminal*. Ipak, potrebno je istaći da između digitalnog, internet i sajber kriminala postoje suštinske konceptualne razlike, pri čemu je potonji pojam bliži onome što domaće zakonodavstvo u Zakonu o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala prepoznaje i normativno definiše kao visokotehnološki kriminal.

(McGuire & Dowling, 2013: 5). Drugu grupu kriminalnih radnji vezanih za sajber prostor čine one vrste kriminaliteta koje se mogu odvijati i bez upotrebe informaciono-komunikacionih sistema, ali njihovom upotrebom dobijaju na obimu i dometu (2013: 6). U ovu grupu svrstavaju se radnje kao što su različite vrste prevara (fišing mejlovi, prevare prilikom e-kupovine i vršenja bankarskih transakcija), krađa ličnih podataka, trgovina ljudima, ilegalnim supstancama i robom, maltretiranje (eng. *cyberbullying*) i drugo.

Ekonomski parametri potvrđuju strahove da je sajber kriminalitet sve izraženiji izazov za moderna društva. Njegova ukupna vrednost pre samo jedne decenije procenjivana je na približno 450 milijardi američkih dolara (Reuters, 2014), dok se trenutne procene kreću i do 10 biliona dolara (Virtasant, 2025), što ukazuje na dramatičan porast i značajan uticaj ovog fenomena na globalnom nivou. Slične trendove moguće je identifikovati i u Srbiji, gde je, prema podacima Vrhovnog javnog tužilaštva (VJT RS), u periodu od 2014. do 2024. godine zabeležen porast broja predmeta iz oblasti visokotehnološkog kriminala od čak 508% (VJT RS, 2025: 27). Najzastupljenija krivična dela u tom kontekstu uključuju ugrožavanje sigurnosti, proganjanje, neovlašćeno prisluškivanje i snimanje, kao i prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (VJT RS, 2025: 30). Ovakva struktura krivičnih dela u velikoj meri korespondira sa trendovima uočenim u komparativnim istraživanjima drugih država (Abdullah & Jahan, 2020: 95).

Posebno istaknuti aspekti sajber kriminaliteta jesu njegova anonimnost i transnacionalnost što je veoma izraženo, kako u državnim statističkim podacima (VJT RS, 2025: 28), tako i u medijski pokrivenim incidentima, čak i onda kada su u pitanju državne institucije i sa njima povezani incidenti kao što su slučajevi Elektroprivrede Srbije (Baletić, 2024) ili Republičkog geodetskog zavoda (Dragojlo & Tešić, 2022). Nesposobnost državnih institucija da izađu na kraj sa novim tehnološkim izazovima u vidu sajber kriminaliteta otvara „novo polje socijalne anksioznosti" (Ungar, 2001: 271) odlikovano nepredvidivošću, nekontrolisanošću i specifičnim tipom medijskog izveštavanja (Moore, 2013: 41). Rizici povezani sa sajber prostorom postali su individualizovani čime je svaki pojedinac postao nosilac značajne odgovornosti (2013: 41). Ova se odgovornost ogleda u horizontalnoj i vertikalnoj umreženosti pojedinca čija nepažnja može narušiti bezbednost drugih sajber aktera sa kojima je povezan što dovodi do daljeg porasta troškova saniranja posledica sajber kriminaliteta (Krivokapić,

Nikolić, & Živković, 2023: 1404). Kao posebno destruktivni po kompanije i institucije pokazali su se napadi koji su izvedeni direktno od strane državnih sajber aktera ili grupa koje deluju uz njihovu posrednu podršku (Autor, 2025a: 305), jer su izazivali značajnu ekonomsku štetu i ozbiljno narušavali normalno funkcionisanje državnog aparata (Autor, 2025b: 227). Izloženost apstraktnim, a veoma opasnim, rizicima na koje tradicionalni mehanizmi zaštite i kontrole, pre svega u vidu prinudnih mera kojima raspolaže država, ne daju dobre rezultate, postavlja edukaciju kao jedna od efikasnijih načina izgradnje sveukupne otpornosti društva.

3. Medijsko izveštavanje o sajber kriminalitetu: specifičnosti i izazovi

Sajber kriminalitet doživljava stalnu evoluciju, kako u vrstama učinjenih dela, tako i u metodama njihovog izvršenja, čime su pojedinci prinuđeni da se stalno informišu i usvajaju nova znanja kako i sami ne bi postali žrtve. Zato se sve češće u fokusu medijskog izveštavanja mogu naći različite taktike za identifikovanje potencijalnih pretnji i podizanje lične bezbednosti u sajber prostoru. Međutim, podjednako važno sa kao i širenjem znanja o novim pretnjama jeste i privlačenje pažnje javnosti i prenošenje informacije načinom komunikacije razumnljivim široj populaciji, što u slučaju sajber bezbednosti može predstavljati izazov (Ahmad, Abd Mubin, & Arzeman, 2023: 525). Potreba da se privuče pažnja publici do koje je teško doći usled ogromne produkcije informacija utiče na izbor vesti iz oblasti sajber kriminala, stavljajući fokus na velike slučajeve kao što su napadi na institucije, kompanije ili poznate ličnosti čime se gubi iz vida da ovi akteri najčešće imaju resurse i mehanizme da umanje ili uklone nanetu štetu, ali i da oni čine tek neznatan deo žrtava sajber kriminala (Abdugofforov, 2024: 5).

Medijska prezentacija sajber kriminaliteta, usled svojih specifičnih karakteristika, iziskuje prilagođavanje novinarskih tehnika i načina interpretacije događaja. Dok se tradicionalne forme kriminaliteta vezuju za određeni prostor i vizuelne prezentacije kao što su mesto zločina, oružje, fotografije i identitet žrtava, svedoka ili učesnika, sajber kriminalitet se odvija u apstraktnom prostoru u kome pojedinci ili organizacije neretko i nisu svesni da su postali žrtve. Ilustrativan primer razlika između fizičkog i sajber kriminaliteta jeste krađa: u fizičkom svetu ona podrazumeva trajno oduzimanje predmeta od vlasnika, dok

u virtuelnom prostoru krađa često ne podrazumeva otuđenje u svakodnevnom poimanju, već kopiranje, umnožavanje ili neovlašćeni pristup informaciji bez gubitka originala (Jewkes & Linnemann, 2017: 355).

Odsustvo uobičajenih vizuelnih asocijacija na kriminal ima važne posledice po način na koji mediji izveštavaju o sajber kriminalitetu. S obzirom na to da je sajber prostor po svojoj prirodi apstraktan i u značajnoj meri lišen vizuelnih elemenata, interpretacija informacija i generisanje vesti o ovom fenomenu uglavnom su ograničene na nekolicinu državnih institucija i stručnih organizacija koje raspolažu potrebnim ekspertizama (Krasnay, 2024: 3). Takođe, objavljivanje informacija o sajber napadima u kojima su institucije ili kompanije žrtve može im naneti ozbiljnu reputacionu štetu zbog čega one često izbegavaju da priznaju da su se takvi incidenti dogodili ili da je nastala određena šteta (Sangari, Dallal & Whitman, 2022). Usled ovih faktora, broj relevantnih izvora informacija je znatno manji nego kod tradicionalnog kriminaliteta. Ovako izražena informaciona asimetrija dovodi do toga da mediji imaju sužene mogućnosti za samostalnu proveru dobijenih informacija, što otvara prostor za širenje spekulacija i neproverenih tvrdnji u informacionom prostoru. Ograničena sposobnost medija, a posredno i šire javnosti, da pristupe pouzdanim i proverenim informacijama o sajber kriminalitetu posebno dolazi do izražaja u slučajevima kada su mete napada državne institucije, koje često nastoje da umanje obim ili značaj incidenata radi zaštite svog autoriteta i sprečavanja širenja panike (Peljto & Stjepanović, 2024; Krivokapić, Nikolić, & Živković, 2023: 1408). Međutim, netransparentnost institucija prilikom izveštavanja o posledicama sajber incidenata može dovesti do neslaganja sa ekspertskom zajednicom, izuzetno osetljivom na ovakve rizike, što će biti razjašnjeno u narednim delovima rada.

Tradicionalni načini izveštavanja nalaze se pred značajnim izazovom u vidu, sve zastupljenijeg, sajber kriminaliteta koji svojim karakteristikama otežava njegovu medijsku prezentaciju. Ograničena dostupnost pouzdanih informacija, potreba za privlačenjem pažnje javnosti i prilagođavanje sadržaja čitaocu kroz pojednostavljivanje informacija su samo dodatni izazovi koji ne samo što otežavaju prenošenje vesti od medija do korisnika već utiču i na kreiranje distorzirane slike sajber okruženja. Pomenuti izazovi izrazito negativno utiču na sposobnost medija da ispune jedan od svojih osnovnih ciljeva, edukaciju javnosti, koja je u kontekstu sve nebezbednijeg sajber prostora krucijalna. U situaciji u kojoj pojedinci ne mogu da se oslone na državne institucije i njihovu pretnju silom,

edukacija i preventivno delovanje postaju glavni stubovi sajber bezbednosti i društvene otpornosti na ovakve pretnje, dok kvalitetno medijsko izveštavanje zauzima poziciju glavnog izvora primera pozitivnih praksi i praktičnih saveta. U takvom kontekstu, uloga medija prevazilazi osnovnu, informativnu funkciju i postaje strukturni deo odgovora društva na nove bezbednosne izazove digitalnog doba.

4. Metodologija

Analiza članaka na internet portalima kroz prizmu teorije uokviravanja predstavlja ustaljen pristup u ispitivanju načina na koji mediji oblikuju i prenose narative svojoj publici (videti: Semetko & Valkenburg, 2000; Jevtić, 2025; Yi, Liu &Yang, 2024). Iako postoje sporenja oko definicije uokviravanja kao teorijskog pristupa analizi narativa, oko ovog koncepta razvila se živa istraživačka tradicija sa izuzetnom akademskom produkcijom (Lecheler & de Vreese, 2019: 2). Entmen (eng. *Robert Mathew Entman*) ističe da se uokviravanje u medijskom prostoru može analizirati kroz prisustvo ili odsustvo ključnih reči ili fraza, izvora informacija ili učestalih stereotipnih slika koje pojačavaju utisak određenih sudova i činjenica na čitaoca (1993: 52). Drugim rečima, okviri imaju selektivnu funkciju: oni naglašavaju određene aspekte stvarnosti, stavljajući ih u prvi plan, dok istovremeno potiskuju druge (Lecheler & de Vreese, 2019: 5). Uokviravanje je kontinuirani proces koji se odvija zasebno u svakoj fazi kreiranja i interpretiranja informacija, od autora vesti i medija do samog čitaoca (Dahinden, 2006: 13). U fokusu ovog istraživanja nalazi se analiza narativnih okvira koje pojedini mediji primenjuju u izveštavanju, a koji su identifikovani u sadržajima objavljenim na njihovim internet portalima. Jedan od najšire primenjivanih i metodološki utemeljenih pristupa proučavanju medijskog uokviravanja (videti: Lecheler & de Vreese, 2019; Matthes & Kohring, 2004) predstavlja analizu osnovnih narativnih okvira prema tipologiji koju su ponudili Semetko (eng. *Holli Semetko*) i Valkenburg (eng. *Patti Valkenburg*). Kao osnovni okviri identifikovani su okvir konflikta, koji ističe sukobe između različitih aktera (država, grupa ili pojedinaca); okvir ljudskog interesa koji se fokusira na neposrednom iskustvu pojedinaca koji često podrazumevaju važne životne događaje; okvir ekonomskih posledica naglašava finansijske aspekte događaja koji se obrađuje sa različitih nivoa (pojedinac, zajednica, država ili globalno); okvir moralnosti koji za cilj ima izazivanje potrebe za donošenjem

određenih vrednosnih sudova povodom konkretnih događaja i okvir pripisivanja odgovornosti u kome se utvrđuju uzroci i posledice određenih pojava, kao i akteri kojima se pripisuje odgovornost ili uticaj na njihov tok (Semetko & Valkenburg, 2000: 95–100).

Rad se zasniva na kvalitativnoj i kvantitativnoj analizi tekstova koji se bave pitanjem sajber kriminaliteta objavljenih od strane tri medija na njihovim internet portalima: Radio-televizija Srbije (RTS), Kurir i Danas. Kao referentni period za prikupljanje vesti uzet je trogodišnji period od 24. februara 2022. godine, kada je započet rat u Ukrajini čija je sajber dimenzija privukla značajnu pažnju medija, do 24. februara 2025. godine. Ovi portali su odabrani uzimajući u obzir njihovu posećenost, broj vesti koji se bavi pitanjima sajber kriminaliteta, odnosa prema trenutnom političkom poretku (kritičari trenutne vlasti, podržavaoci trenutne vlasti i nominalno neutralni akter) i razlikama koje postoje u stepenu poverenja (videti: Kleut et al, 2022) koje građani imaju prema ovim medijima. Dodatan razlog zašto je Radio-televizija Srbije obuhvaćena istraživanjem jeste njegov specifičan karakter kao medijskog servisa u državnom vlasništvu sa velikim brojem korisnika i visokim stepenom poverenja građana (Kleut et al, 2022).

Selekcija vesti rađena je u dva koraka. U prvom koraku prikupljene su sve vesti koje u svom naslovu, podnaslovu ili prvom pasusu sadrže neki od ključnih pojmova definisanih od strane Lija Dževisa (eng. *Lee Jarvis*) i Stjuarta Mekdonalda (eng. *Stuart Macdonald*) kao najučestalije korišćenih u komunikaciji naučne zajednice i medija u pogledu rizika i pretnji sajber prostora: sajber kriminal, digitalni kriminal, hakerski napadi, sajber napadi, sajber bezbednost, internet prevare i fišing (Jarvis & Macdonald, 2014), kao i pojmovi internet kriminal i visokotehnološki kriminal, koji su prisutni u domaćim medijima. U drugom koraku, vesti koje su se odnosile na promociju knjiga, najavu televizijskih i radio emisija su elimisane iz uzorka. Takođe, ukoliko u tekstu vesti sajber kriminalitet ne figurira kao centralna tema, ta vest je takođe izbačena iz uzorka. Prilikom kodiranja, u obzir su uzimani naslov, podnaslov i tekst vesti, dok su ostali sadržaji kao što su fotografije, video ili audio materijali i komentari izostavljeni iz analize. Kako bi rezultati kodiranja bili kvalitetni, izvršeno je merenje Holstijevog koeficijenta pouzdanosti obračunom unutrašnje i međukoderske pouzdanosti (Mao, 2017). Rezultati su bili zadovoljavajući, s obzirom da se vrednost koeficijenta kretala u rasponu od 0.85 do 1.00, u zavisnosti od posmatrane kategorije.

Istraživanje je obuhvatilo 222 vesti sa portala RTS-a (n=61), Danasa (n=63), i Kurira (n=98). Podaci koji su kodirani u istraživanju su: a) da li se vest odnosi na sajber kriminalitet u Srbiji, u regionu Zapadnog Balkana, na globalnom nivou ili vesti nisu geografski određene; b) izvor informacija na osnovu kojih je vest produkovana (eksperti, nedržavni akteri, državne institucije, drugi mediji, redakcija medija i drugo); c) prisustvo informacija i saveta koji su usmereni ka edukaciji čitaoca i d) prisustvo određenih narativnih okvira u vesti. Dalje, prikupljeni podaci su podvrgnuti kvantitativnoj i kvalitativnoj analizi kako bi se identifikovale dominantne teme, uočile medijske pristrasnosti i ocenile razlike u načinu izveštavanja između posmatranih medija.

5. Rezultati

1) Kvantitativna i tematska analiza medijskog izveštavanja o sajber kriminalitetu

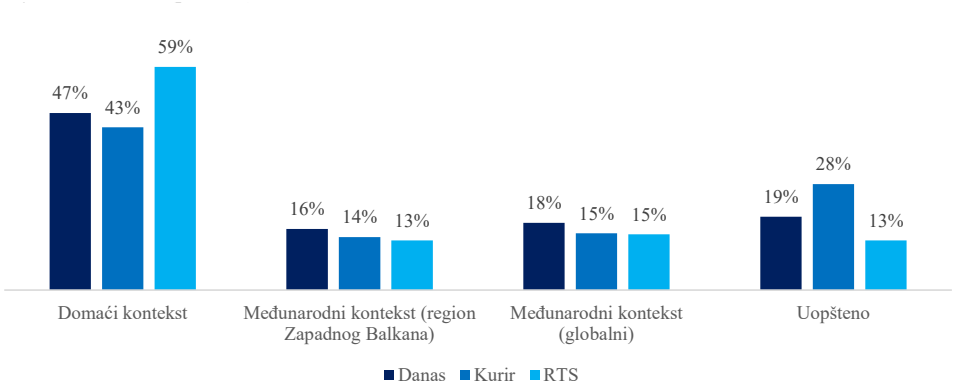
Jedna od prvih uočljivih razlika između analiziranih medijskih portala ogleda se u kvantitetu sadržaja posvećenog temi sajber kriminaliteta. Naime, ova tema je najzastupljenija na portalu Kurir, koji se u medijskoj literaturi često povezuje sa senzacionalističkim pristupom izveštavanju (Kleut, 2022: 6). Nasuprot tome, portali RTS i Danas, koji se češće povezuju sa umerenijim stilom izveštavanja, beleže približno jednak broj tekstova na ovu temu. Ova kvantitativna razlika prisutna je i u pogledu tematskog fokusa: dok Kurir prevashodno izveštava o internet prevarama, govoru mržnje i hakerskim napadima sa međudržavnim karakterom, drugi posmatrani mediji se češće bave širim spektrom sajber rizika.

Prilog 1: Tematska zastupljenost vesti u ukupnom uzorku

Na nivou celokupnog uzorka, najzastupljenije kategorije vesti (Prilog 1) odnose se na konkretne forme sajber kriminaliteta, kao što su internet prevare, govor mržnje i ilegalna trgovina, koje se javljaju kao dominantna tema u 19% posmatranih tekstova, kao i hakerski napadi na institucije (takođe 19%), svrstavajući u ovu kategoriju incidente koji su se dogodili u Srbiji i inostranstvu. Iako se izveštavanje sva tri posmatrana medija odlikuje umerenim tonom, naslovi predstavljaju tačku razdvajanja između ovih medija. S jedne strane, RTS i Danas zadržali su umerenost u izražavanju i u formulisanju naslova, dok se, s druge strane, Kurir često služi velikim slovima, alarmističkim i senzacionalističkim formulacijama kako bi izazvao emocionalnu reakciju čitalaca i privukao ih samim naslovom. Izrazi kao što su „šok“ (*Kurir*, 03. maj 2024), „ratnici iz senke“ (*Kurir*, 03. mart 2023), „u opasnosti ste“ (12. jun 2024.) ili „hitno ažurirajte sve“ (*Kurir*, 14. septembar 2023.) tipični su primeri ovakvog pristupa, usmerenog na stvaranje dramatičnosti i povećanje čitanosti.

Pored toga, relativno visok nivo učestalosti (>10%) imaju vesti koje čitaocima pružaju konkretne savete o zaštiti u sajber prostoru (15%). Ovakvi sadržaji ukazuju na tendenciju medija da deo pažnje usmere ka praktičnim aspektima sajber bezbednosti, kroz savete koji se najčešće odnose na bezbednu internet kupovinu, prepoznavanje fišing napada, kreiranje i čuvanje kvalitetnih lozinki, kao i zaštitu osetljivih podataka poput onih sa ličnih dokumenata ili kreditnih kartica. Relativno značajnu zastupljenost u uzorku čine vesti o sajber napadima između država, kao i one koje sajber kriminalitet posmatraju uopšteno, ukazu-

jući na rastuću pretnju, bez direktnog upućivanja na konkretne slučajeve sajber incidenata (po 13%).



Prilog 2: geografska raspodela vesti posmatrana kroz pojedinačne medije

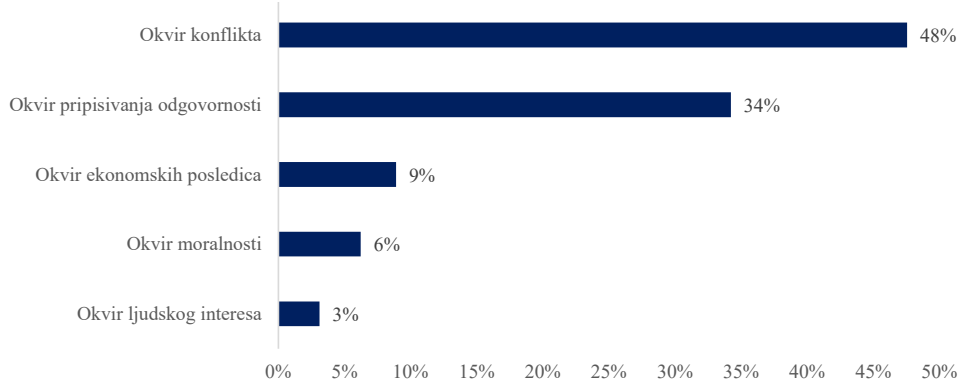
Sa aspekta geografske raspodele (Prilog 2), pažnja medija dominantno je usmerena na slučajeve sajber kriminaliteta koji su se dogodili na teritoriji Srbije pa tako je RTS u 59%, Danas u 47%, a Kurir u 43% tekstova stavljaju fokus na lokalne incidente. Sa druge strane, podaci ukazuju na relativno ujednačenu zastupljenost vesti koje su usmerene na regionalne i globalne događaje: sadržaji koji se odnose na Zapadni Balkan obuhvataju između 13% i 16% svih vesti, dok se tekstovi koji se odnose na incidente van posmatranog regiona javljaju u intervalu od 15% do 18%. Najzastupljenije teme u okviru ovih kategorija obuhvataju sajber rat između Ukrajine i Rusije, što ilustruju naslovi poput „Ruski hakeri izvršili više od hiljadu sajber napada na Ukrajinu od početka invazije“ (Kurir, 2023) i „Rusi izveli hakerski napad koji se ne pamti: zove se napad ‘bližeg suseda’, zbunjeni i stručnjaci“ (Kurir, 2023). Takođe, značajnu zastupljenost u medijima dobila su i dva značajna incidenta iz regiona Zapadnog Balkana, kada su institucije u Crnoj Gori i Albaniji pretrpele sajber napade avgusta i septembra 2022. godine kojima im je onemogućeno normalno funkcionisanje narednih nekoliko meseci (Autor, 2025b: 231-232). Ovi tekstovi često sadrže izjave zvaničnika koji se fokusiraju na proces identifikacije aktera odgovornih za sajber incidente što neretko dovodi do optužbi drugih država za njihovu umešanost. Međutim, za razliku od slučajeva Albanije i Crne Gore, gde su visoki državni funkcioneri ubrzo nakon hakerskih napada javno optužili Rusiju i Iran

kao odgovorne, u izveštavanju o sličnim incidentima u Srbiji identifikovano je odsustvo problematizacije potencijalne odgovornosti drugih država i izjava visokih državnih zvaničnika. Umesto toga, odgovornost se redovno pripisuje anonimnim, nezavisnim hakerskim grupama vođenim nepoznatim motivima.

Analiza tematske i geografske strukture izveštavanja o sajber kriminalitetu u tri posmatrana medija ukazuje na značajne razlike u uredničkim pristupima, stilu izveštavanja i izboru izvora. Najveći broj tekstova registrovan je na portalu Kurir, koji ne samo da teme sajber kriminaliteta tretira učestalije, već ih obrađuje kroz prizmu senzacionalističkog i često alarmističkog diskursa kao što su „Hitno ažurirajte sve!“ (*Kurir*, 14. septembar 2024), „Za manje od 60 sekundi "probiju" naše lozinke!“ (*Kurir*, 20. jun 2024.) ili „Ako dobijete ovakvu poruku ni slučajno nemojte da klikćete“ (*Kurir*, 22. jun 2024.). Nasuprot tome, RTS i Danas nude uravnoteženiji i manje emotivno obojen pristup, mada sa različitim akcentima: RTS se oslanja na institucionalne izvore i afirmativni narativ prema državnim institucijama, dok Danas zastupa kritičkiji stav, zahteva odgovornost nadležnih institucija i češće angažuje nedržavne aktere kao izvore informacija.

Različite uredničke politike ovih medija uočljive su i sa aspekta geografskih fokusa vesti. Pre svega, broj vesti koji ne sadrži jasno definisanu geografsku odrednicu na koju se vest odnosi (13% kod RTS-a, 19% kod Danasa i čak 28% u Kuriru) pokazuje značajne varijacije između različitih medija u pogledu njihovih fokusa u izveštavanju. Tekstovi bez geografskih odrednica najčešće imaju edukativni karakter, ukazujući čitaocima na primere dobrih praksi u sajber prostoru ili ih upozoravaju na nove oblike sajber pretnji, poput fišing napada, krađe podataka ili pojave novih zlonamernih softvera. Sa druge strane, medijskim sadržaj posvećen sajber bezbednosti i kriminalitetu predominantno je usmeren na teritoriju Srbije. Istovremeno, domaći incidenti se najčešće tretiraju kao tehnički problemi, bez šire političke implikacije. Ukupno posmatrano, strukturalni i tematski izbori analiziranih medija upućuju na različite pozicije unutar medijskog prostora, ali i na različite interpretacije značaja, prirode i društvenog konteksta sajber kriminaliteta.

2) Medijski diskurs u izveštavanju o sajber kriminalitetu



Prilog 3: zastupljenost medijskih okvira u ukupnom uzorku

Sprovedena analiza medijskog diskursa o sajber kriminalitetu otkriva izrazitu zastupljenost okvira konflikta (Prilog 3), koji je identifikovan u 48% posmatranih novinskih članaka. Ovakav rezultat ukazuje na sklonosti medijskih aktera da sajber kriminalitet konceptualizuju primarno kroz paradigmu antagonističkih odnosa između različitih aktera, pri čemu posebnu ulogu imaju narativi o međudržavnim sajber napadima u kontekstu različitih sukoba, a posebno rusko-ukrajinskog konflikta, čije posledice osećaju i države na Zapadnom Balkanu. Drugi najčešće zastupljen medijski okvir jeste okvir pripisivanja odgovornosti, identifikovan u 34% slučajeva, čija sadržinska analiza ukazuje na dominaciju poruka usmerenih na podizanje svesti građana o rizicima koje nosi sajber prostor i taktikama kako se njihova bezbednost može podići. Važno je istaći da određen broj vesti identifikovanih u okviru pripisivanja odgovornosti usmeren ne samo prema građanima, već i prema državnim institucijama, kao nosiocima sistemske odgovornosti za zaštitu od pretnji sajber kriminaliteta. U poređenju sa do sada pomenutim medijskim okvirima, ostali posmatrani okviri pokazuju značajno nižu zastupljenost: ekonomski okvir prisutan je u 9% uzorka, moralni okvir u 6%, dok je okvir ličnih iskustava najmanje prisutan sa 3%. Ovakvi rezultati pokazuju da u medijskom predstavljanju sajber kriminaliteta preovlađuje konfrontacioni model, uz značajno prisustvo narativa koji u prvi plan stavlja odgovornost pojedinaca za sopstvenu bezbednost u sajber okruženju. Istovremeno, moguće je uočiti zanemarivanje vesti usmerenih na

lična iskustva i pitanje etičke dimenzije sajber kriminala, što ukazuje na dominaciju tehnicističkog viđenja sajber bezbednosti u kome pretnju predstavljaju nevidljivi, dehumanizovani akteri. Pretnja se najčešće doživljava kao anonimna, permanentna i stalno evoluirajuća, na čije negativne efekte ni pojedinci ni institucije nisu imuni.

Sajber napadi na institucije predstavljali su učestao predmet medijskog izveštavanja, sa udelom u ukupnom korpusu koji se kreće između 21% i 26%, u zavisnosti od medija. Međutim, pristup ovoj temi značajno varira u zavisnosti od generalnog odnosa određenog medija prema vladajućoj partiji u Srbiji. Kurir i RTS, kao prodržavni i državni medij, akcenat stavljaju na narativ koji rad državnih institucija posmatra pozitivno, ističući njihovu efikasnost, odgovorno postupanje, bezbednost građana i ograničenost štete nastale kao posledice hakerskih napada. Nasuprot tome, Danas generiše znatno negativniju sliku rada državnih organa, ističući sistemsku ranjivost, nedostatak transparentnosti u radu državnih organa i izostanak političke odgovornosti za nastalu štetu. Razlika u fokusu dodatno se oslikava u činjenici da Kurir i RTS u potpunosti izostavljaju pitanje odgovornosti institucija, što ukazuje na jasno izražen vrednosni jaz u odnosu na Danas, koji zauzima kritičkiji stav prema državnim institucijama i trenutnoj državnoj politici bezbednosti u sajber prostoru.

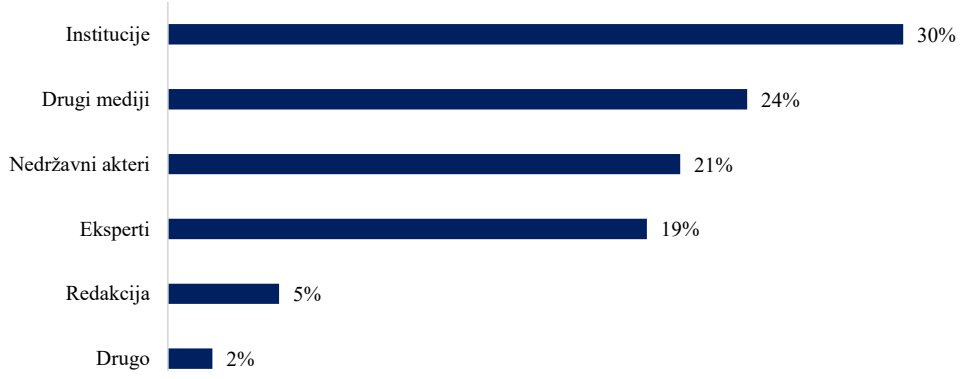
3) Obrazovna dimenzija medijskog izveštavanja

Pored informisanja javnosti o događajima koji se odvijaju u zemlji i inostranstvu, mediji imaju i važnu edukativnu ulogu, naročito kada je reč o novim i nepoznatim fenomenima kao što je sajber kriminalitet, koji je podložan stalnim promenama i inovacijama. Upravo zbog toga, jedan od značajnijih aspekata izveštavanja u analiziranim medijima odnosi se na tekstove sa edukativnom funkcijom, čiji je cilj da čitaocima pruže konkretne i primenljive savete u oblasti lične sajber bezbednosti. Takvi sadržaji se mogu kategorizovati u dve osnovne grupe: (1) tekstovi koji obrađuju individualne slučajeve žrtava sajber kriminaliteta sa ciljem upozoravanja publike (Moore, 2013: 37), kojima su u pogledu narativnih okvira najbliži okvir ljudskog interesa i (2) tekstovi u kojima autori daju opšte smernice o odgovornoj upotrebi interneta i zaštiti ličnih podataka, stavljući fokus na odgovornosti pojedinaca za sopstvenu bezbednost.

Najveći broj ovakvih tekstova zabeležen je na portalima Kurir i RTS, gde čine značajan deo ukupne produkcije na temu sajber kriminaliteta – 26% u

slučaju Kurira i 23% u slučaju RTS-a. Nasuprot tome, Danas je znatno manje posvećen kreiranju ovakvog sadržaja, sa udelom od samo 8%. Sličan trend je uočljiv i kada je reč o tekstovima koji imaju karakter preventivnog upozoravanja, tj. onima koji javnost obaveštavaju o novim oblicima pretnji. Takvi tekstovi se najčešće formulišu u obliku pitanja ili senzacionalističkih naslova, što je posebno izraženo kod Kurira. Naslovi poput „Na ovom mestu nikada ne punite telefon – razlog će vas šokirati!" imaju za cilj da privuku pažnju i izazovu osećaj urgentnosti, dok istovremeno ukazuju na rizike povezane s sajber nebezbednošću. Iako su ovakvi naslovi retorički efektni, njihova forma otvara pitanje balansa između informisanja i emocionalne manipulacije, što može uticati na percepciju pretnje i kod informisane i kod manje informisane publike.

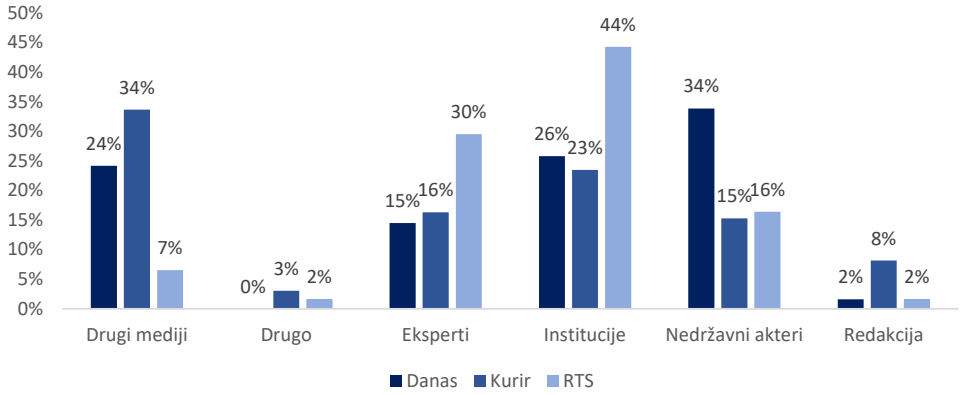
4) Izvori informacija i njihov značaj u kreiranju medijskog diskursa



Prilog 4: izvori informacija prikzani u ukupnom uzorku

Struktura izvora na kojima mediji zasnivaju svoje izveštavanje predstavlja ključni indikator uredničke politike i profesionalne orijentacije medija. Ukupna analiza posmatranih novinskih članaka (Prilog 4) pokazuje da se najveći broj tekstova oslanja na informacije koje dolaze od institucija (30%), zatim od drugih medija (23%), nedržavnih aktera poput predstavnika civilnog sektora ili privatnih kompanija (21%), kao i od ekspertske zajednice (19%). Međutim, kada se posmatraju pojedinačni mediji (Prilog 5), uočavaju se značajne razlike. Danas u najvećoj meri koristi nedržavne aktere kao primarni izvor informacija (34%), što korespondira sa njegovom kritički orijentisanom uredničkom pozicijom prema

državnim institucijama i trenutnom političkom poretku. Pored toga, Danas često koristi i državne institucije (26%) i druge medije (24%) kao izvore podataka, mahom kada su u pitanju vesti u vezi sajber kriminaliteta van granica Srbije, što pak ukazuje na relativno raznovrsnu izvornu bazu informacija.



Prilog 5: izvori informacija prikazani za svaki analizirani mediji pojedinačno

S druge strane, Kurir se najviše oslanja na tekstove preuzete iz drugih medija (34%), ali i na zvanične izjave predstavnika državnih institucija (23%). Takav izbor izvora podataka podržava narative koji su bliski institucionalnom diskursu i često su usklađeni s narativom koji favorizuju predstavnici institucija i aktuelne vlasti. Ovo je posebno izraženo prilikom izveštavanja o domaćim sajber incidentima u čijem središtu se nalaze institucije, gde se kao neosporni autoritet uzimaju izjave njihovih predstavnika. U izveštavanju RTS-a, kao javnog servisa u državnom vlasništvu, dominiraju informacije dobijene direktno od državnih organa (44%) i eksperata (30%), što ukazuje na institucionalni autoritet kao ključni oslonac informativne politike, ali i podršku narativima promovisanim od strane državnih organa, posebno u kontekstu slučajeva sajber kriminaliteta koji su se dogodili na teritoriji Srbije.

Ova razlika u tipologiji izvora potvrđuje ranije uočene ideološke i strukturne razlike među medijima. Dok RTS i Kurir pokazuju veću zavisnost od institucionalnih izvora, što može biti povezano sa njihovim pozicioniranjem bliže državnim strukturama unutar šire medijske scene u Srbiji, Danas nastoji da obezbedi kritički distanciran pristup kroz oslanjanje na aktere izvan državnog

aparata koji su znatno skloniji kritikama državne politike. Upravo ovaj izbor izvora utiče i na ton i sadržaj medijskog izveštavanja, što se ogleda u različitim pristupima interpretacije pojava kao što su sajber napadi, bezbednosne pretnje ili odgovornost institucija. Takva urednička selekcija izvora ne samo da reflektuje unutrašnje vrednosne orijentacije medija, već i aktivno oblikuje okvire kroz koje publika doživljava i tumači ključne društvene i bezbednosne procese. Takođe, razlika u strukturi izvora ukazuje na moguće distinkcije u percepciji relevantnosti i ozbiljnosti problema u vidu sajber kriminaliteta, pri čemu se incidenti van Srbije predstavljaju kao pitanje nacionalne bezbednosti od najvišeg značaja, dok se domaći incidenti tretiraju prevashodno kao tehnički ili administrativni problemi ograničenog političkog dometa.

6. Diskusija

Iako primenjene metode kvalitativne i kvantitativne analize pružaju uvid u postojeće medijske narative, određena ograničenja prisutna u istraživanju moraju biti naglašena. Prvovenstveno, analizom su obuhvaćena samo tri medija, što ograničava mogućnost generalizacije zaključaka na celokupno medijsko polje u Srbiji u kontekstu izveštavanja o sajber kriminalitetu. Drugo, analiza je obuhvatila isključivo tekstualne sadržaje, dok su drugi elementi, a posebno oni multimedijalni, poput slika i video priloga, izostavljeni, iako mogu značajno uticati na percepciju vesti i dodatno unaprediti kvalitet analize. Analiza komentara povezanih sa posmatranim vestima, kako na samim portalima, tako i na profilima ovih medija na društvenim mrežama takođe može pružiti dodatne uvide u percepciju građana o ovom važnom pitanju.[4] Fokus na vremenski period od 2022. do 2025. godine obezbeđuje relevantnost, ali otežava kreiranje šire istorijske analize medijske produkcije vesti o sajber kriminalitetu i dominantnih narativa. Sa ciljem unapređenja kvaliteta dobijenih uvida neophodno je sprovesti longitudinalnu analizu kako bi se pratili trendovi u predstavljanju sajber kriminaliteta kroz duži vremenski period.

Još jedan potencijalni pravac budućih istraživanja jeste poređenje izveštavanja u nacionalnim i regionalnim medijima, kao i analize medijskih diskursa u drugim kulturološkim kontekstima, što bi omogućilo bolje razumevanje globalnih i lokalnih razlika u percepciji sajber bezbednosti. Iako postoje komparativ-

[4] Primer dobrog istraživanja na polju analize komentara čitalaca internet portala: https://aseestant.ceon.rs/index.php/comman/article/view/48963/26983

na istraživanja koja analiziraju medijske diskurse u sajber okruženju u različitim nacionalnim kontekstima (videti: Mazrouei, Čigoja Piper, & Connolly, 2022; Silva, Raposo de Mello, & Nishijima, 2022), većina njih akcenat stavlja na sajber bezbednost kao centralnu temu istraživanja, dok je sajber kriminalitet do sada retko bio razmatran kao centralni analitički pojam.

7. Zaključak

Sajber kriminalitet, kao jedan od najdinamičnijih i najmanje opipljivih fenomena savremenog društva, postavlja brojne izazove ne samo donosiocima političkih odluka i državnim institucijama, već i svim građanima pojedinačno, koji su sve izloženiji rizicima koji potiču iz sajber okruženja. U takvom kontekstu, uloga medija kao jednog od ključnih posrednika u distribuciji informacija i izgradnji društvene svesti o sajber pretnjama postaje izuzetno važna. Takav trend izuzetno je vidljiv i u Srbiji, gde su razlike u odnosima posmatranih medija prema trenutnom političkom poretku uočljive čak i u tumačenju sajber kriminaliteta i pretnje koju od predstavlja za društvo i institucije. Dublja analiza vesti na portalima RTS-a, Kurira i Danasa ukazuje da narativi dominantni u vestima o sajber kriminalitetu ne odsupaju od ukupne uređivačke politike ovih medija, već predstavljaju njihov kontinuitet.

Najveća zastupljenost vesti o sajber kriminalitetu, koja je identifikovana na portalu Kurira, ovom problemu pristupa uz izražen senzacionalizam, podržavajući poruke i narative kreirane od strane države, prenoseći dominantne karakteristike svoje uredničke politike i na ovo polje. Nasuprot tome, RTS i Danas pokazuju uravnoteženiji pristup temi, pri čemu je RTS orijentisan ka institucionalnim izvorima i afirmativnom predstavljanju državih institucija, dok Danas pristupa sajber kriminalitetu uz veći oslonac na nedržavne aktere kao važan izvor informacija i uz značajnu kritiku države politike, njene netransparentnosti i nedostatak odgovornosti među njenim predstavnicima. Ove razlike ukazuju na postojanje dubokih vrednosnih i političkih razlika u medijskom pristupu sajber temama, ali i na različite ciljne grupe koje svaki od ovih medija nastoji da informiše. Razlike u pristupu problemu sajber kriminaliteta izuzetno su vidljive prilikom izveštavanja o sajber incidentima koji uključuju državne institucije u Srbiji i inostranstvu. Za medije u kojima dominiraju narativi koji podržavaju postojeći politički poredak u Srbiji, hakerski napadi usmereni prema njenim institucijama u velikoj meri predstavljeni su kao minorni bezbednosni incidenti

iza kojih stoje nepoznate i neimenovane hakerske grupe. Sa druge strane, u slučajevima napada na institucije u drugim državama, pretnja se percipira kao značajna, a izveštavanje obuhvata i izjave visokih državnih zvaničnika i motive napadača koji su često povezani sa drugim državama. Takav pristup stvara asimetričnu sliku o prirodi sajber pretnji u kojoj je domaći sajber prostor znatno bezbednije okruženje, što se može negativno odraziti na svest građana o postojećim rizicima. Istovremeno, veliki broj tekstova koji nemaju geografsku odrednicu ili se fokusiraju na davanje saveta za ličnu zaštitu, svedoči o interesovanju medija za obrazovnu dimenziju izveštavanja, što je naročito važno u uslovima individualizovane odgovornosti za sajber bezbednost.

Izvori informacija koje mediji koriste dodatno osvetljavaju razlike u profesionalnom i ideološkom profilu posmatranih medija. Dok se Kurir najviše oslanja na druge medije i državne zvaničnike, RTS dominira u korišćenju institucionalnih i ekspertskih izvora, a Danas pridaje veći značaj nedržavnim akterima kao opoziciji dominantnim institucionalnim porukama. Upravo izbor izvora utiče na ton, strukturu i okvir u kome je neki događaj predstavljen, čime se medijski narativi konstituišu kao proizvodi ne samo informacionog nego i vrednosnog procesa. Rezultati istraživanja jasno ukazuju da mediji u Srbiji, iako sve više prepoznaju značaj sajber bezbednosti kao društvenog prioriteta, i dalje nisu u potpunosti prilagodili svoje izveštavanje specifičnostima sajber kriminaliteta. Senzacionalizam, fokus na velike slučajeve i nedovoljna kritička distanca prema institucionalnim izvorima otežavaju kvalitetno i pouzdano informisanje javnosti od strane značajnog dela medija u Srbiji. Međutim, postoje i pozitivni pomaci, pre svega u značajnom broju tekstova usmerenih ka pružanju praktičnih saveta, kao i većeg angažovanja eksperata u objašnjavanju apstraktnih i javnosti nedovoljno poznatih pojava i tema iz oblasti sajber kriminaliteta.

Mediji u velikoj meri doprinose oblikovanju javne percepcije sajber kriminaliteta, ali ta uloga nosi odgovornost koja je specifična u odnosu na onu koju su mediji posedovali kada su u pitanju tradicionalni vidovi kriminaliteta. Ukoliko je cilj izveštavanja izgradnja društvene otpornosti na rizike koje sa sobom nosi sajber prostor, neophodno je da se novinarska praksa u ovoj oblasti oslobodi senzacionalizma, temelji na stručnim i proverenim izvorima, i više angažuje u edukaciji javnosti. Samo takav pristup može doprineti izgradnji bezbednosne kulture u digitalnom dobu, u kojoj mediji poseduju ne samo informativnu, već i preventivnu i edukativnu ulogu.

Literatura

Abdugofforov, I. (2024). „Media narratives and misconceptions on cybercrime". *Journal of Cyber Law*, Vol 1 (1), 1–5.

Abdullah, A. T. M., & Jahan, I. (2020). „Causes of cybercrime victimization: A systematic literature review". *International Journal of Research and Review*, Vol 7 (5), 101–113.

Ahmad, Z. A., Abd Mubin, N. N., & Arzeman, A. (2023). „Content analysis of cybercrime infographic". *Jurnal Komunikasi: Malaysian Journal of Communication*. Vol. 39 (4), 523–541.

Al Mazrouei, M. K., Čigoja Piper, D., & Connolly, L. Y. (2022). "Beware of titles: Analysing media reporting of cybercrime in UK and UAE". In *Proceedings of the 2022 Cyber Research Conference – Ireland (Cyber-RCI)*, 1–5.

Baletić, K. (2024, December 19). Serbian public still in the dark over 2023 energy utility hack. *Balkan Insight*. Dostupno na adresi: balkaninsight.com/2024/12/19/serbian-public-still-in-the-dark-over-2023-energy-utility-hack/.

Banović, B., & Ilić, A. (2019). „Mediji i organizovani kriminalitet". u Kostić, J., & Stevanović, A. (ur.) *Finansijski kriminalitet i korupcija*, Vršac: Institut za uporedno pravo i Institut za kriminološka i sociološka istraživanja, 157-169.

Autor. (2025). „Sajber napadi kao strategijski instrument spoljne politike: Zapadni Balkan u eri hibridnog rata". u Blagojević, V. i Subotić, M. (ur), Geostrateška budućnost Balkana. Beograd: Institut za međunarodnu privredu i politiku i Institut za strategijska istraživanja, 223 – 245.

Autor. (2025). „The influence of non-state cyber actors in conventional armed conflicts: a case study of the War in Ukraine", in S. Blagojević & D. Trifković (eds), *VojNa 2025: International scientific conference on military sciences*, Belgrade: Military Academy, 304-310.

Boholm, M. (2021). „Twenty-five years of cyber threats in the news: A study of Swedish newspaper coverage (1995–2019)". *Journal of Cybersecurity*, Vol 7 (1), 1-23.

Buse, C., & Meißner, F. (2019). *Much ado about hacking? How news media in Germany, the United Kingdom, and the United States report cyber threats*. Media and Communication, Vol 7(1), 104-115.

Dahinden, U. (2006). „Framing: An integrative theory of mass communication science". Konstanz, UVK.

Dhasmana, S., Mishra, S. K., Upadhyay, A., & Gond, S. K. (2024). „Investigating cybercrime news reporting in Indian online news media". *Library Progress International*, Vol 44 (3), 210–214.

Donalds, C., & Osei-Bryson, K.M. (2019). „Toward a cybercrime classification ontology: A knowledge-based approach". *Computers in Human Behavior,* Vol 92, 403–418.

Dragojlo, S., & Tešić, A. (2022, September 21). Hackers likely accessed emails of Serbia's cadastre staff, BIRN reveals. *Balkan Insight*. Dostupno na adresi: balkaninsight.com/2022/09/21/hackers-likely-accessed-emails-of-serbias-cadastre-staff-birn-reveals/.

Entman, R. B. (1993). "Framing: Toward clarifcation of a fractured paradigm". *Journal of Communication*, Vol 43, 51 – 58 .

Gomes, S., Sardá, T., & Granja, R. (2022). „Crime, justice and media: Debating (mis)representations and renewed challenges". *Comunicação e Sociedade*, Vol 42, 7–24.

Greer, C. (2013). „Crime and Media: Understanding the Connections" in C. Hale, K. Hayward, A. Wahadin and E. Wincup (eds.). *Criminology*, third edition, Oxford: Oxford University Press. 25–45.

Happer, C., & Philo, G. (2013). „The role of the media in the construction of public belief and social change". *Journal of Social and Political Psychology*, Vol 1 (1), 321–336.

Ilić, A. (2017). *Mediji i kriminalitet – kriminološki aspekti* (doktorska disertacija). Univerzitet u Beogradu: Pravni fakultet.

Jarvis, L., & Macdonald, S. (2014). „Locating cyberterrorism: How terrorism researchers use and view the cyber lexicon". *Perspectives on Terrorism,*Vol 8 (2), 52–65.

Jewkes, Y., & Linnemann, T. (2017). *Media and crime in the U.S.*, 2nd edition. Washington DC: SAGE Publications.

Kleut, J. (2022). *Mapping disinformation in Serbian media 2020*. CRTA.

Kleut, J., Ninković Slavnić, D., Ilić, V., Išpanović, I. (2022). *Report on digital news in Serbia*. Novi Sad: Independent Journalists' Association of Vojvodina.

Krasznay, C. (2024). "The role of civilian cybersecurity companies in military cyber operations". *Land Forces Academy Review*, Vol 29 (1), Article 113, 1-14.

Krivokapić, Đ., Nikolić, A., & Živković, I. (2023). „Capacities of Western Balkan economies (and their public sectors) to respond to ransomware attacks". In *Proceedings of the 46th International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1403–1408).

Krstić, A., Milojević, A., & Kleut, J. (2018). „Vizuelno uokviravanje protesta *Protiv diktature*". *CM: Communication and Media*, Vol XIII (44), 57–92.

Lecheler, S., & de Vreese, C. H. (2019). *News framing effects*. London: Routledge.

Mao, Y. (2017). „Intercoder reliability techniques: Holsti method". ин M. Allen (Ed), *The SAGE encyclopedia of communication research methods*. Washington DC: SAGE Publications, 741–743.

Matthes, J., & Kohring, M. (2004). „The empirical measuring of media frames". *Medien & Kommunikationswissenschaft*, Vol 52 (1), 56–75.

McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence. Summary of key findings and implications* (Home Office Research Report 75). Home Office Science.

Milutinović, I., Pavlović, J. (2019). „Diskurs o nasilju prema ženama u srpskim onlajn medijima: dominantne komunikacijske strategije". CM: Communication and Media, Vol XIV (45), 5-36.

Moore, S. E. H. (2013). „The cautionary tale: A new paradigm for studying media coverage of crime". in C. Critcher, J. Hughes, J. Petley, & A. Rohloff (Eds), *Moral panics in the contemporary world*, London: Bloomsbury Academic, 33–50.

Peljto, S., & Stjepanović, J. (2024, January 22). Sistem EPS-a posle hakerskog napada funkcioniše, ali nije bezbedan. *Bloomberg Adria*. Dostupno na adresi: https://rs.bloombergadria.com/politika/opste/50561/sistem-eps-a-posle-hakerskog-napada-funkcionise-ali-nije-bezbedan/news.

Rader, E., & Wash, R. (2015). „Identifying patterns in informal sources of security information". *Journal of Cybersecurity*, Vol 1 (1), 121–144.

Sandle, P. (2014, June 9). Cyber crime costs global economy $445 billion a year: Report. *Reuters*. Dostupno na adresi: reuters.com/article/technol-

ogy/cyber-crime-costs-global-economy-445-billion-a-year-report-idUSKBN0EK0SV/.

Sangari, S., Dallal, E., & Whitman, M. (2022). „Modeling under-reporting in cyber incidents". *Risks*, Vol 10 (11), Article 200, 1-14.

Semetko, H. A., & Valkenburg, P. M. (2000). "Framing European politics: A content analysis of press and television news". *Journal of Communication*, Vol 50 (2), 93-109.

Silva, M. G. T., Raposo de Mello, A. C., & Nishijima, M. (2022). T"raditional written media coverage and cybersecurity events: The NSA case". *Revista do CESOP,* Vol 28 (1), 268–291.

Skopik, F., Settanni, G., & Fiedler, R. (2016). "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing". *Computers & Security*, Vol 60, 154–176.

Stošić, L. V., & Janković, A. V. (2022). „Cybercrime in the Republic of Serbia: Prevalence, situation and perspectives". *Kultura polisa,*Vol: 19 (4), 82–99.

Trajković, J. (2020). „Predstavljanje osoba sa invaliditetom u srpskoj štampi: Analiza dnevnih novina Blic i Danas". *CM: Communication and Media*, Vol XV (47), 85-108.

Ungar, S. (2001). „Moral panic versus the risk society: The implications of the changing sites of social anxiety". *The British Journal of Sociology*, Vol 52 (2), 271–291.

United Nations. (2000). *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10–17 April 2000*. United Nations.

Virtasant. (2025, March 10). Cybercrime costs skyrocket to $10.5 trillion: AI in cybersecurity fights back. Dostupno na adresi: virtasant.com/ai-today/cybercrime-costs-skyrocket-to-10-5-trillion-ai-in-cybersecurity-fights-back.

Vrhovno javno tužilaštvo Republike Srbije. (2024). *Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2024. godini*. VJT RS.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Cambridge: Polity Press.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Službeni glasnik Republike Srbije, br. 61/2005, 104/2009 10/2023 i 10/2023 – dr. zakon.

Aleksandar Bogićević
Institut za strategijska istraživanja, Beograd

MEDIA AND CYBERSECURITY: REPRESENTATION OF CYBERCRIME IN THE SERBIAN DIGITAL SPACE

Abstract: *Relying on the application of framing theory, a content analysis was conducted on 222 news articles published between February 2022 and February 2025 on three online platforms: RTS (the national public broadcaster), Kurir (tabloid daily), and Danas (a critically oriented media outlet). The articles were coded according to thematic focus, geographic scope, information sources, presence of educational content, and dominant journalistic frames. The study aims to examine how Serbian media construct representations of cybercrime and to what extent these representations may contribute to either the education or the misinformation of the public regarding this important issue. The findings indicate that cybercrime is most frequently framed through conflict and responsibility attribution, with particular emphasis on inter-state cyberattacks in the context of the conflict in Ukraine. Domestic cases, however, are often portrayed as technical incidents of limited political significance. It is important to note that, although educational content aimed at raising individual awareness of cyber security is present, it is often overshadowed by alarmist and simplified reporting. The study concludes that, despite recognising the growing significance of cyber threats, the observed Serbian media have not yet fully adapted their reporting to the complexities of cybercrime. The preference for sensationalism and institutional narratives over critical engagement may lead to a distorted public perception of cyber security. Nevertheless, the identified presence of preventive and educational messages highlights the potential of the media as a significant component of societal resilience in the digital age.*

Keywords*: Cybercrime, Media discourse, Cyber security, Serbia, Societal resilience*