VODIČ
DIGITALNA BEZBJEDNOST - NAJBOLJE PRAKSE

MEDIJSKA ASOCIJACIJA JUGOISTOČNE EVROPE

AUTOR: VUK MARAS

MASE

Reporting Digital Rights & Freedoms

Funded by the European Union

VODIĆ

DIGITALNA BEZBJEDNOST - NAJBOLJE PRAKSE

Autor: Vuk Maras

Oktobar 2025. godine

O autoru

Vuk Maraš ima preko 20 godina iskustva u radu sa medijima u Crnoj Gori i regionu. Bio je programski direktor MANS-a baveći se monitoringom i analitikom sprovođenja zakona i funkcionisanja institucija, a nakon toga obavljao je funkciju izvršnog direktora MASE. Od 2023. godine nalazi se na funkciji izvršnog direktora BIRN Crna Gora.

Učestvovao je u izradi seta medijskih zakona u Crnoj Gori kao i prve Medijske strategije. Autor je brojnih analiza i izvještaja za različite organizacije u Crnoj Gori, regionu i šire.

Izdavač: Medijska Asocijacija Jugoistočne Evrope
Trg Nezavisnosti BB, 81000 Podgorica
www.masee.org

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of MASE and do not necessarily reflect the views of the EU.

MASE

Reporting Digital Rights & Freedoms

Funded by the European Union

UVOD

Digitalna bezbjednost postaje jedno od najvažnijih pitanja za rad medija u Crnoj Gori. Novinari i čitave redakcije sve češće se suočavaju s pokušajima digitalnih upada, sajber napadima i raznim rizicima po bezbjednost podataka. Iako savremene tehnologije omogućavaju bržu i efikasniju komunikaciju, one istovremeno otvaraju prostor za nove vrste prijetnji – od DDoS napada i phishing poruka, do pokušaja nadzora komunikacije i lažnog predstavljanja. Medijska asocijacija Jugoistočne Evrope (MASE) sprovela je tokom oktobra 2025. godine anketu među crnogorskim medijima kako bi sagledala stvarno stanje digitalne bezbjednosti, postojeće kapacitete i prakse reagovanja u slučaju napada. Anketom je obuhvaćeno 21 medij različitog profila – od internet portala i televizija, do radija i štampanih medija. Digitalne prijetnje realna su svakodnevnica crnogorskih medija, a razumijevanje i ublažavanje tih prijetnji ključno je za opstanak slobodnog novinarstva.

Ovaj vodič predstavlja nalaze istraživanja i analize MASE o digitalnoj bezbjednosti medija, uz osvrt na širi kontekst digitalnih prava i sloboda. U narednim poglavljima razmatra se zbog čega je digitalna sigurnost od suštinskog značaja za slobodu izražavanja, koji su najvažniji rizici i izazovi sa kojima se medijske kuće suočavaju, te koje najbolje prakse su dosad prepoznate u redakcijama.

Takođe, vodič nudi preporuke za unapređenje sistema zaštite i predlaže model implementacije mjera čija održivost treba da obezbijedi trajnu otpornost medija na sajber prijetnje. Krajnji cilj ovog dokumenta je da pomogne crnogorskim novinarima i urednicima da bolje razumiju digitalne opasnosti i da usvoje efikasne strategije odbrane, čuvajući pritom osnovne vrijednosti novinarstva i slobode izražavanja.

SADRŽAJ

1.
KONTEKST I ZNAČAJ DIGITALNE BEZBJEDNOSTI

U eri ubrzane digitalne transformacije, zaštita medija na internetu postala je neizostavan dio borbe za slobodu izražavanja i pravo javnosti da bude informisana. Digitalna prava i slobode danas predstavljaju sastavni dio osnovnih ljudskih prava u virtuelnom prostoru. Međutim, u društvu poput crnogorskog, sa izraženim političkim podjelama i tenzijama, digitalni kanali komunikacije sve više se zloupotrebljavaju za podsticanje i širenje dezinformacija, govora mržnje, pa čak i sukoba i nasilja. Dezinformacione kampanje i strani uticaji nameću ozbiljne izazove crnogorskom društvu, dok nedovoljni mehanizmi zaštite omogućavaju ugrožavanje državne bezbjednosti i digitalnih sloboda. To se manifestuje kroz povrede privatnosti, širenje mržnje i online pozive na nasilje, koji direktno ili posredno utiču i na medije kao izvore informacija.

Brz razvoj digitalnih medija donio je medijima u Crnoj Gori brojne prednosti, omogućivši im bržu razmjenu informacija i globalnu dostupnost sadržaja. Ipak, taj razvoj sa sobom nosi i nove izazove: isti ti digitalni kanali otvaraju nove metode napada na vitalne interese društva, olakšavaju plasiranje propagande i lažnih vijesti, te omogućavaju narušavanje bezbjednosti na načine koji ranije nijesu postojali. U takvim uslovima, zaštita slobode izražavanja dobija dodatno na značaju – ne samo za novinare i medije, već i za svakog građanina koji danas može da objavi informaciju u online sferi. Istovremeno, mogućnost zloupotrebe tog prava danas je veća nego ikada, jer digitalna infrastruktura omogućava brzu i anonimnu distribuciju sadržaja koji može nanijeti štetu drugima.

Važno je naglasiti da digitalna bezbjednost medija nije samo tehničko pitanje informacione tehnologije, već i profesionalno pitanje koje direktno utiče na slobodu izražavanja, zaštitu izvora i integritet novinarstva.

Drugim riječima, ako novinari ne mogu bezbjedno komunicirati i čuvati svoje podatke, ugrožena je i sama suština novinarske profesije.

Crnogorski propisi prepoznaju značaj ove teme: doneseni su ključni zakoni (npr. Zakon o informacionoj bezbjednosti, Zakon o tajnosti podataka,) i strategije (Strategija sajber bezbjednosti 2022–2026 i sl.) koje se bave unapređenjem sajber otpornosti. Planirano je osnivanje i Agencije za sajber bezbjednost sa ciljem da štiti mrežne i informacione sisteme od sajber prijetnji i da nadzire primjenu mjera bezbjednosti.

Ipak, pored normativnog napretka, i dalje postoje veliki praznini u praksi: Crna Gora i dalje nema adekvatne mehanizme za pravovremeno detektovanje sajber napada, kao ni za dovoljno brz odgovor i oporavak nakon incidenata. Takođe, hronično nedostaje stručnjaka za sajber bezbjednost, što je problem koji je globalno prisutan, a u maloj zemlji poput naše još izraženiji.

Ovakva situacija otežava zaštitu onlajn prostora od zloupotreba i ostavlja medije i građane izloženim štetnim sadržajima. S druge strane, svaka mjera ograničavanja digitalnog sadržaja nosi i rizik cenzure, pa je neophodno pažljivo uspostaviti ravnotežu između zaštite bezbjednosti i očuvanja slobode govora. Upravo zbog te ravnoteže, rad digitalnih medija i platformi treba regulisati tako da se istovremeno štiti sloboda izražavanja, ali i osigura odgovornost za plasirane informacije – da se suzbije govor mržnje i namjerne dezinformacije, a da se ne ugrozi kritičko novinarstvo.

2.
KLJUČNI RIZICI I IZAZOVI

Istraživanje MASE iz oktobra 2025. potvrdilo je da su crnogorski mediji u značajnoj mjeri izloženi sajber rizicima. Čak 15 od 21 anketiranog medija (odnosno 71%) izjavilo je da je u proteklih godinu dana bilo meta nekog oblika digitalnog napada. Samo pet redakcija (24%) navelo je da *nijesu* bile napadnute u tom periodu, dok je jedan učesnik ankete kazao da nije siguran da li je bilo napada.

Ovi podaci nedvosmisleno ukazuju da su napadi na medije česti, te da gotovo nijedna redakcija nije pošteđena rizika. Priroda tih napada varira: najčešće prijavljeni oblici su distribuirani napadi uskraćivanja usluge (DDoS) koji obaraju medijske sajtove, zatim phishing poruke kojima se pokušava ukrasti pristup ili instalirati zlonamjerni softver, kao i koordinisane dezinformacione kampanje protiv medija. Pored toga, zabilježeni su i pokušaji lažnog predstavljanja (npr. slanje lažnih mejlova u ime novinara ili urednika) i upadi u naloge na društvenim mrežama redakcija. Neke redakcije prijavile su čak i pokušaje nadzora njihove interne komunikacije ili krađe osjetljivih korisničkih podataka. Ovakav spektar prijetnji pokazuje da opasnosti dolaze sa različitih strana – od tehnološki sofisticiranih "hakerskih" napada, do informacionih manipulacija usmjerenih na narušavanje ugleda medija.

Napadi nijesu ravnomjerno raspoređeni po učestalosti: većina medija navodi da se incidenti dešavaju relativno *rijetko*, tek povremeno ili otprilike jednom godišnje. Ipak, najmanje tri medija su prijavila da su pod napadima praktično svakog mjeseca, što znači da su određene redakcije kontinuirano na meti i djeluju u uslovima visokog rizika.

Takva konstantna izloženost može biti povezana sa profilom tih medija, moguće je da se radi o redakcijama koje redovno objavljuju istraživačke priče ili osjetljive informacije koje nekome smetaju.

U skladu s tim, istraživanje je identifikovalo i glavne ciljeve napada: u 43% slučajeva napadači nastoje da onemoguće rad medijskog sajta ili IT sistema, dakle da ućutkaju medij privremenim gašenjem njegovih platformi. Otprilike trećina napada ima za cilj kompromitaciju reputacije medija (33%), širenjem lažnih informacija ili diskreditacijom, dok oko 10% napada očigledno ima špijunski karakter – praćenje komunikacije novinara i redakcija.

Iz toga se može zaključiti da sajber napadi na medije uglavnom nijesu slučajni niti puki čin sajber vandalizma, već svrsishodne akcije s jasnom namjerom da se utiče na rad novinara. Često je cilj da se medij ućutka ili zastraši, pogotovo ako objavljuje sadržaje od javnog interesa koji nekome mogu zasmetati.

Pored direktnih tehnoloških napada, mediji se suočavaju i sa širim digitalnim izazovima koji utiču na njihov rad. Dezinformacione kampanje predstavljaju jedan od najčešćih vidova pritiska na medije – čak 38% ispitanih redakcija prepoznalo je upravo organizovano širenje lažnih vijesti ili lažno predstavljanje kao vrlo čestu prijetnju. Takve kampanje mogu poticati iz centara propagande, uključujući i strane aktere, s ciljem da se oslabi povjerenje javnosti u profesionalne medije ili da se skrene pažnja sa nezgodnih tema. Govor mržnje je takođe značajan problem u onlajn sferi Crne Gore – novinari i mediji nerijetko postaju mete koordinisanih uvreda i prijetnji na društvenim mrežama zbog svog izvještavanja. Ove pojave stvaraju atmosferu pritiska i autocenzure, što je takođe oblik ugrožavanja digitalnih sloboda.

Istovremeno, postoje stotine neregistrovanih internet portala i anonimnih naloga na mrežama koji plasiraju neprovjerene informacije i targetiraju legitimne medije. Pravni okvir još uvijek ne obavezuje takve online platforme na transparentnost i odgovornost, pa one djeluju izvan standardnih mehanizama kontrole. Analiza MASE iz aprila 2025. ukazuje da je neophodno definisati odgovornost upravo tih neregistrovanih portala i uvesti sankcije za širenje sadržaja koji nisu zaštićeni slobodom govora. Dok se to ne

uredi, profesionalni mediji ostaju izloženi nelojalnoj konkurenciji i kampanjama kojima je cilj da ih diskredituju ili zbune publiku.

Još jedan ozbiljan izazov jeste nedostatak povjerenja između medija i državnih institucija kada je riječ o sajber bezbjednosti. Istraživanje je pokazalo da većina napadnutih medija (oko 70%) svoje incidente uopšte nije prijavila nadležnim organima. Učesnici ankete kao razloge za neprijavljivanje najčešće navode nepovjerenje u to da bi institucije adekvatno reagovale ili zaštitile medij, zatim neznanje kome se tačno obratiti, ali i osjećaj da nemaju dovoljno dokaza o počiniocima. Samo manji broj ispitanika kazao je da je pokušao kontaktirati državne organe ili sajber stručnjake, ali bez jasnog odgovora ili korisne povratne informacije. Ovakav raskorak između medijskog sektora i institucija dodatno pogoršava situaciju: napadi ostaju u sivoj zoni, počinioci nekažnjeni, a mediji prepušteni sami sebi da se snalaze. Dugoročno, takva situacija podriva vladavinu prava u digitalnom prostoru i ohrabruje nove napade, jer napadači računaju na nekažnjivost.

Na kraju, treba pomenuti da prijetnje digitalnoj bezbjednosti medija dolaze ponekad i iz samih struktura koje bi trebalo da štite društvo. Primjer toga je slučaj nezakonitog nadzora komunikacija iz 2020. godine: protiv bivšeg direktora Agencije za nacionalnu bezbjednost (ANB) u toku je krivični postupak zbog zloupotrebe položaja, tačnije zbog nezakonitog prisluškivanja i nadzora političara, sveštenika i novinara u tom periodu.

Ti navodi pokazuju da su čak i novinari bili predmet tajnog nadzora od strane bezbjednosnih službi, što predstavlja grubo kršenje prava na privatnost i slobodu medija. U drugom slučaju masovnog kršenja digitalnih prava, vlasti su početkom pandemije 2020. objavile spisak imena građana u samoizolaciji – uključujući njihove lične podatke – što je Ustavni sud kasnije ocijenio kršenjem ustavnog prava na privatnost. Iako ovaj primjer nije neposredno vezan za medije, on ilustruje ambijent u kom djeluju: nedovoljno razvijena kultura zaštite podataka i privatnosti može lako dovesti i do ugrožavanja novinarskih izvora ili komunikacija. Sve navedeno potvrđuje da se mediji u Crnoj Gori nalaze u složenom digitalnom okruženju gdje im, pored tehničkih sajber napada i online kampanja, prijetnje predstavljaju i sistemski propusti i zloupotrebe.

3.
NAJBOLJE PRAKSE I ISKUSTVA REDAKCIJA

Iako je slika izazova zabrinjavajuća, istraživanje MASE pokazuje i da među crnogorskim medijima raste svijest o potrebi unapređenja digitalne bezbjednosti. Mnoge redakcije su posljednjih godina počele preduzimati konkretne korake kako bi zaštitile svoju digitalnu infrastrukturu, podatke i novinare na terenu.

Na pitanje da li imaju uspostavljene interne procedure za postupanje u slučaju sajber napada, odgovori su bili podijeljeni u tri jednaka dijela: sedam medija (33%) je navelo da ima razvijene interne protokole i smjernice za digitalnu bezbjednost, sedam (33%) priznaje da takve procedure nema, dok preostalih sedam (33%) kaže da ih sprovodi djelimično, odnosno da imaju poneka pravila ali ne i zaokružen sistem. Ovakvi rezultati ukazuju da postoji određeni nivo svijesti i inicijative, jer je trećina medija već uvela neko interno pravilo ili politiku radi zaštite (što se može smatrati dobrom praksom), dok još jedan dio to radi djelimično.

No, u isto vrijeme, veliki broj redakcija nema nikakav formalizovan plan reagovanja na digitalne incidente, što znači da se oslanjaju na ad hoc rješenja i ličnu snalažljivost novinara i urednika, odnosno IT osoblja ako ga imaju, ako do napada dođe.

Pozitivno je to što se sve veći broj novinara edukuje o digitalnoj bezbjednosti. Skoro polovina ispitanih medija (10 od 21) navela je da su njihovi novinari ili IT osoblje prošli neku vrstu obuke iz ove oblasti. Još četiri medija planiraju da organizuju takve obuke u

narednih godinu dana, dok sedam (33%) nema nikakvih planova po tom pitanju.
Dakle, može se reći da je barem u polovini redakcija prepoznata potreba stručnog usavršavanja kadra za prepoznavanje i odbranu od digitalnih prijetnji. Novinari tradicionalno nijesu tehnički specijalisti, ali najbolja praksa savremenog novinarstva nalaže bar osnovnu digitalnu pismenost: prepoznavanje phishing emaila, korišćenje sigurnih lozinki i enkriptovanih kanala komunikacije, provjera izvora informacija na internetu, itd.

Oni mediji koji su već uložili u obuku zaposlenih sada imaju određenu prednost – njihovo osoblje svjesnije je opasnosti i vještije u korišćenju alata za zaštitu podataka. MASE istraživanje ipak naglašava da znatan broj redakcija i dalje nema ni osnovna znanja o zaštiti podataka, bezbjednom korišćenju komunikacionih kanala i prepoznavanju digitalnih prijetnji. To znači da će kontinuirane obuke biti neophodne kako bi se ovaj jaz u znanju premostio.

Kada je riječ o tehničkim kapacitetima, istraživanje je utvrdilo da otprilike polovina medija ima određen nivo podrške u slučaju sajber incidenta. Preciznije, 11 medija (52%) izjavilo je da može računati na internu IT službu ili eksternog stručnjaka koji bi pomogao ako dođe do digitalnog napada. Šest medija (29%) ima djelimičnu podršku, što znači povremeni pristup nekom IT stručnjaku ili ograničene resurse, dok četiri medija (19%) uopšte nemaju nikakvu tehničku pomoć te vrste.

Ovi brojevi reflektuju realnost da veće redakcije, koje imaju više zaposlenih i bolje finansije, uglavnom mogu priuštiti IT osoblje ili ugovorni servis, dok mali lokalni mediji najčešće nemaju koga da pozovu u slučaju krizne situacije. Upravo to potvrđuju i odgovori u anketi – veće redakcije, sa svojim IT sektorom ili eksternim partnerom, mnogo lakše odgovaraju na digitalne prijetnje, dok manji mediji ostaju bez pomoći kada su najranjiviji.

Kao dobru praksu možemo izdvojiti primjere medija priključili globalnim mrežama za zaštitu (npr. korišćenje usluga poput Cloudflare za odbranu od DDoS napada). Iako takve inicijative nijesu eksplicitno pomenute u izvještaju, poznato je u regionalnoj medijskoj zajednici da neki vodeći portali koriste napredne servise

zaštite upravo zbog učestalih napada. Za manje medije, međutim, troškovi takvih servisa mogu biti prepreka, zbog čega oni najčešće ostaju na osnovnoj zaštiti.

Kada se posmatra opšti nivo digitalne bezbjednosti medija, samopercepcija ispitanih redakcija govori mnogo. Prosječna ocjena kojom su mediji ocijenili nivo svoje digitalne bezbjednosti iznosi 2,9 od 5, što znači da ukupno gledano vlada tek umjeren nivo zaštite.

Zanimljiv je podatak da nijedan medij sebi nije dao najvišu ocjenu (5/5) po tom pitanju, čime su posredno priznali da su svjesni postojećih slabosti. Kao najčešće zaštitne mjere koje redakcije primjenjuju navedeni su antivirusni i firewall sistemi, sigurno čuvanje lozinki (korišćenje password managera ili čestih izmjena lozinki), a u nešto manjoj mjeri i dvofaktorska autentifikacija za pristup nalozima.

To su osnovne higijenske mjere digitalne bezbjednosti koje svaki medij danas treba da ima. Ipak, istraživanje otkriva da vrlo malo redakcija ima uspostavljene politike redovnih bezbjednosnih provjera (poput periodičnih IT audita) ili automatizovane rezervne kopije podataka na sigurnom mjestu. Ovo su naprednije prakse koje zahtijevaju dodatne resurse i znanje, pa ne čudi što nijesu rasprostranjene. Izostanak redovnih provjera znači da mnogi mediji možda i nijesu svjesni svih svojih ranjivosti dok ne bude prekasno, a nepostojanje automatskih backupova nosi rizik gubitka dragocjenih podataka u slučaju ozbiljnog napada (primjera radi, ransomware napada koji bi enkriptovao podatke redakcije).

Iskustva samih redakcija, prikupljena kroz otvorena pitanja u anketi, osvjetljavaju konkretne probleme i potrebe na terenu. Više učesnika istraživanja naglasilo je potrebu za dodatnim obukama zaposlenih, posebno novinara koji nijesu tehnički potkovani, kao prioritetnu stavku. To potvrđuje da su mediji svjesni kako ljudski faktor često predstavlja najslabiju kariku u lancu bezbjednosti – novinar koji ne prepozna sumnjiv email ili koristi slabu lozinku može nenamjerno otvoriti vrata napadačima. Dalje, istaknut je nedostatak finansijskih sredstava za nabavku naprednih zaštitnih softvera i tehničke opreme.

Budžeti medija u Crnoj Gori su ograničeni, pogotovo u lokalnim sredinama, pa izdvajanju za digitalnu sigurnost često nedostaje prostora. Redakcije su ukazale i na nepostojanje jasnog kanala komunikacije s državnim institucijama kada je u pitanju sajber bezbjednost. Drugim riječima, kada se napad desi, mediji ne znaju tačno kojoj državnoj službi da prijave incident niti od koga mogu očekivati pomoć ili savet, što se poklapa sa ranije navedenim nalazom o neprijavljivanju napada.

Konačno, učesnici ankete primijetili su porast spam pošte i lažnih poruka koje stižu sa domaćih i inostranih servera. To implicira da je protok zlonamjernog sadržaja u elektronskoj komunikaciji u ekspanziji, čineći svakodnevni rad novinara sve zamornijim i složenijim (jer iz mora mejlova treba izlučiti one legitimne od potencijalno opasnih).

Zbirno posmatrano, iskustva crnogorskih redakcija govore o tome da su one na "prvoj liniji" odbrane slobode izražavanja u digitalnom dobu, često prepuštene same sebi da se nose sa nadolazećim prijetnjama. Istraživanje MASE jasno pokazuje da sajber prijetnje postaju sve češće, dok su kapaciteti medija da na njih odgovore i dalje ograničeni. Ova disproporcija između sve jačih napada i nedovoljnih odbrambenih mehanizama znači da je medijskom sektoru potreban sistemski iskorak ka boljoj zaštiti. Prosječna ocjena ispod 3 od 5, uz činjenicu da dvije trećine medija nema kompletne interne procedure, potvrđuje hitnost uspostavljanja ozbiljnijeg, strateškog pristupa digitalnoj bezbjednosti. Optimizam uliva to što su neki mediji već otpočeli pozitivne prakse: obučavaju osoblje, uvode osnovne mjere zaštite i dijele međusobno iskustva o napadima. Ali, da bi te prakse postale standard, potreban je širi podsticaj i podrška, kako unutar same branše, tako i od države i stručne zajednice.

4.
PREPORUKE ZA UNAPREĐENJE SISTEMA

Da bi se odgovorilo na postojeće izazove, neophodno je djelovati na više nivoa, od same medijske industrije, preko državnih institucija, do šire društvene zajednice. MASE je u svom izvještaju iz oktobra 2025. ponudio konkretne preporuke usmjerene na jačanje digitalne otpornosti medija u Crnoj Gori.

Prije svega, potrebno je razviti nacionalni program za jačanje digitalne otpornosti medija, koji bi na strateški način okupio relevantne aktere i obezbijedio finansijsku i tehničku podršku za unapređenje sajber bezbjednosti u novinarskom sektoru. Takav program omogućio bi sistematsku edukaciju, nabavku zaštitnih sredstava i uspostavljanje protokola u svim redakcijama, a posebno bi targetirao one najranjivije – lokalne i male medije.

Kontinuirane obuke i radionice za novinare, urednike i IT osoblje predstavljaju drugu ključnu preporuku. Redovne trening sesije, bilo kroz formalne kurseve ili interne radionice, održavale bi svijest o najnovijim prijetnjama i gradile kulturu preventivne bezbjednosti u redakcijama.

Treća preporuka MASE odnosi se na uspostavljanje jedinstvenog institucionalnog kanala za prijavljivanje digitalnih napada na medije, uz njegovo intenzivno promoviranje među redakcijama. To praktično znači da bi država trebalo da odredi (ili osnuje) tijelo – poput posebne jedinice pri budućoj Agenciji za sajber bezbjednost, kojoj bi mediji mogli odmah prijaviti svaki incident. Taj kanal bi služio i za brz odgovor (npr. tehničku analizu napada) i za prikupljanje dokaza radi eventualnog krivičnog gonjenja počinilaca.

Dalje, preporučuje se da država posebno podrži male i lokalne redakcije kroz grantove i tehničku pomoć namijenjenu unapređenju njihove digitalne bezbjednosti. Takva podrška mogla bi obuhvatiti nabavku osnovnih sigurnosnih alata (licencirani antivirus, firewall uređaje), angažovanje vanjskih IT konsultanata koji bi izvršili procjenu rizika za svaku redakciju, kao i finansiranje naprednih rješenja poput zaštite od DDoS napada za lokalne portale od kritičnog značaja za zajednicu.

Uporedo s tim, digitalnu bezbjednost treba integrisati u programe medijske pismenosti i novinarske obuke. To znači da bi obrazovne institucije, novinarske škole i treninzi za mlade reportere ubuduće morali uključivati i module o sajber bezbjednosti, posebno u dijelu kako zaštititi sopstvene podatke, kako čuvati povjerljivost izvora u digitalnom okruženju, i slično. Time bi nova generacija novinara od početka karijere bila svjesna ovog aspekta novinarstva.

Posebno se ističe značaj međusobne saradnje među medijima: preporučuje se razmjena iskustava i zajednički nastup redakcija kada je riječ o odbrani od napada. U praksi, to bi moglo značiti da mediji međusobno dijele informacije o pokušajima napada (npr. upozorenja o phishing emailovima koji kruže), da veći mediji pruže manjem savjet ili pomoć kada primijete kampanju dezinformacija, ili čak da kolektivno nastupaju prema nadležnima radi zagovaranja boljih uslova zaštite.

Najzad, data je preporuka svim medijskim kućama da razviju interne politike digitalne bezbjednosti – formalne pravilnike koji bi uredili postupanje zaposlenih u online sferi (korišćenje službenih naloga, pravljenje rezervnih kopija, pravila za lozinke, protokol u slučaju napada i dr.). Takve interne politike pomogle bi da se bezbjednosni standardi sprovedu u djelo unutar svake redakcije i da se smanji ljudska greška koja dovodi do incidenta.

Prethodno nabrojane, specifično usmjerene mjere za medije, treba posmatrati i u širem okviru ukupnog jačanja digitalne bezbjednosti i prava u Crnoj Gori. Analiza digitalnih prava i sloboda koju je MASE objavio u aprilu 2025. godine naglašava da unapređenje medijske sajber otpornosti mora biti praćeno unapređenjem pravnog, regulatornog i institucionalnog okvira u državi. U tom

smislu, sajber bezbjednost se mora tretirati i kao pitanje ljudskih prava, a ne samo tehnike - otvoren, slobodan i bezbjedan sajber prostor je u interesu demokratskog društva koliko i u interesu medija. MASE je stoga pozvao na podizanje javne svijesti o tome da je bezbjednost interneta i slobode izražavanja neodvojivo povezana. Istovremeno, pravni okvir i institucije moraju preuzeti veću odgovornost za ponašanje u sajber prostoru. To znači da zakoni trebaju omogućiti djelotvornu zaštitu od online nasilja, diskriminacije i govora mržnje, uz efikasno procesuiranje počinilaca takvih djela. Ključ je pronaći balans: sankcionisati one radnje na internetu koje predstavljaju kriminal (poput poziva na nasilje ili targetiranog govora mržnje), ali izbjeći pretjerano ili nejasno kažnjavanje širenja neistinitih informacija koje ne dostižu prag krivičnog djela. U suprotnom, moglo bi doći do nedozvoljenog ograničavanja slobode izražavanja pod izgovorom borbe protiv "lažnih vijesti".

Takođe, preporučuje se ojačavanje stručnih kapaciteta policije i tužilaštva za suzbijanje sajber kriminala. Bez dovoljno obučenih forenzičara i istražitelja, teško je očekivati da će napadi na medije ikada biti razriješeni ili napadači procesuirani. Državni organi moraju biti u stanju da prate tragove digitalnih zločina, identifikuju počinioce i prikupe valjane dokaze za sudske procese. Povezano s tim, nužno je revidirati i dopuniti postojeće zakone koji se tiču sajber bezbjednosti i digitalnih prava, u skladu s najboljim evropskim standardima. Strateški dokumenti već prepoznaju pravce djelovanja (npr. potrebu da se doradi krivično zakonodavstvo za hibridne prijetnje i dezinformacije), ali tu ideje treba pretočiti u konkretne zakonske izmjene, vodeći računa da se istovremeno očuvaju osnovna ljudska prava. Jedno od takvih unapređenja trebalo bi biti i usklađivanje domaćih propisa o zaštiti podataka sa EU standardima (GDPR), kako bi građani i novinari u Crnoj Gori imali isti nivo zaštite privatnosti kao u Evropskoj uniji. To podrazumijeva i jačanje kapaciteta Agencije za zaštitu ličnih podataka, koja treba da bude kadrovski i tehnički osposobljena da nadzire primjenu tih propisa.

Drugi važan skup preporuka odnosi se na borbu protiv štetnih sadržaja na internetu, a da se pri tom ne ugrozi sloboda medija. Jedan od prioritetnih zadataka je definisanje pojma

"dezinformacija" u zakonu i izrada strategije za borbu protiv namjernog širenja lažnih informacija. Precizno utvrđivanje šta čini dezinformaciju pomoglo bi da se razlikuje zlonamjerno plasiranje laži (npr. od strane botovskih mreža ili propagandnih portala) od običnih grešaka u izvještavanju ili različitih mišljenja, čime bi se omogućilo ciljano suzbijanje onih prvih, a da se ne dira u drugo.

Pored toga, trebalo bi uspostaviti određeni vid institucionalnog nadzora nad online medijskim platformama i propisati sankcije za širenje sadržaja koji ne uživaju zaštitu slobode izražavanja (poput govora mržnje i poziva na nasilje). Ovo je osjetljiva preporuka – nadzor ne smije prerasti u cenzuru, ali regulatorna tijela mogla bi dobiti proširene ingerencije da reaguju kada internet portali objavljuju zaista neprihvatljiv sadržaj. Posebno je problem što mnogi portali nijesu registrovani kao mediji te formalno izmiču svakoj kontroli; tu bi zakonodavac morao pronaći model da ih obuhvati ili da ih sankcioniše ako krše propise. Još jedan važan aspekt je podizanje nivoa znanja i svijesti svih korisnika interneta. Preporuke MASE insistiraju na masovnoj edukaciji, kako građana, tako i novinara, radi većeg stepena njihove bezbjednosti na internetu.

To uključuje kontinuirane javne kampanje kojima bi se građani ohrabrili da prijavljuju incidente (npr. prijave policiji slučajeve online prevara, govor mržnje ili uznemiravanja), zatim obuku građana o zaštiti ličnih podataka i uređaja koje svakodnevno koriste, kao i specifične treninge za novinare o prepoznavanju dezinformacija, propaganda i manipulacija.

Što se medija tiče, uloga njih i njihovih udruženja može biti ključna u promociji medijske pismenosti i digitalnih vještina, kako unutar redakcija tako i prema publici.

Konačno, dugoročni uspjeh mjera zavisi i od saradnje svih društvenih aktera i adekvatne podrške institucija. Potrebno je pojačati koordinaciju između vlade, privatnog sektora (poput IT kompanija, telekomunikacionih operatera), akademske zajednice i civilnog društva, kako bi se pravovremeno i efikasno odgovaralo na sve sajber izazove. To podrazumijeva dijeljenje informacija o prijetnjama u realnom vremenu, zajedničke vježbe simulacije sajber

napada, te uključivanje medija u nacionalne protokole kibernetičke zaštite.

Uporedo, nužno je povećati ulaganja u sajber bezbjednost i to ne samo kroz jednokratne projekte, nego sistemski. Država bi trebala izdvojiti više finansijskih sredstava za uspostavljanje mehanizama ranog otkrivanja sajber prijetnji, brzi odgovor na incidente i oporavak nakon napada.

Bez adekvatnog budžeta, mnoge dobre ideje o kojima je ovdje bilo riječi ne mogu zaživjeti u praksi.

5.
MODEL IMPLEMENTACIJE I ODRŽIVOST MJERA

Uspostavljanje djelotvorne zaštite digitalne bezbjednosti u medijima zahtijeva koordinisan i promišljen pristup. Na osnovu preporuka, može se skicirati model implementacije mjera koji uključuje sve relevantne aktere i predviđa održivost rješenja na duži rok. Centralnu ulogu u koordinaciji trebalo bi da preuzme nadležno državno tijelo – na primjer, Agencija za sajber bezbjednost u saradnji sa Ministarstvom javne uprave ili drugim resornim ministarstvom. Ovo tijelo bi, uz podršku Vlade, pokrenulo izradu nacionalnog programa za digitalnu otpornost medija i okupilo radnu grupu u kojoj bi bili predstavnici medija, medijskih udruženja, eksperti za sajber bezbjednost, predstavnici akademije i relevantnih nevladinih organizacija. Radna grupa bi najprije sprovela detaljnu procjenu trenutnog stanja. Mapirala bi sve medijske kuće, njihove postojeće kapacitete i ključne nedostatke u bezbjednosti. Potom bi se dentifikovali prioriteti: koje redakcije su trenutno najugroženije, koje vrste napada su najčešće, gdje su "rupe" u znanju ili opremi.

Nakon faze procjene, pristupilo bi se planiranju konkretnih aktivnosti. Nacionalni program trebalo bi da definiše niz projekata ili inicijativa: recimo, program kontinuirane obuke novinara (centralizovane radionice na nivou države ili e-learning platforma za samoedukaciju); uspostavljanje sajber centra za pomoć – telefonske linije i online portala gdje mediji mogu prijaviti napad i dobiti savjet u realnom vremenu; dodjelu bespovratnih sredstava (grantova) malim medijima za nabavku sigurnosne opreme ili usluga; izradu priručnika za interne politike bezbjednosti prilagođenog redakcijama; organizovanje godišnje konferencije ili

foruma gdje bi mediji razmjenjivali iskustva o sajber bezbjednosti, uz učešće međunarodnih stručnjaka radi preuzimanja najboljih praksi.

Svaka aktivnost imala bi nosioca (instituciju ili organizaciju zaduženu za realizaciju), vremenski okvir i indikatore uspjeha. Važno je naglasiti ulogu medijskih kuća same: one treba da aktivno učestvuju – da pošalju novinare na obuku, da implementiraju preporučene politike, da otvoreno prijavljuju incidente umjesto da ih kriju. Da bi ih se na to podstaklo, neophodno je graditi povjerenje: državne institucije moraju dokazati da će ozbiljno shvatiti prijave medija i reagovati, umjesto da eventualno zloupotrijebe podatke o napadu za sopstveni marketing ili, u gorem slučaju, nadzor medija.

Implementacija mjera trebala bi biti fazna i fleksibilna. U prvoj godini fokus bi mogao biti na najurgentnijim stvarima: uspostavljanje kanala za prijavu napada i hitne obuke za osnovne digitalne bezbjednosne vještine u svim zainteresovanim redakcijama. Paralelno s tim, pokrenule bi se zakonske inicijative, npr. priprema amandmana na Zakon o medijima ili drugi propisi kako bi se formalizovala obaveza medija da imaju bezbjednosne politike, ili kako bi se definisala odgovornost online platformi.

Druga faza, u naredne dvije do tri godine, obuhvatila bi infrastrukturna ulaganja (nabavka opreme, razvoj softverskih rješenja za monitoring prijetnji) i uspostavljanje održivih struktura – recimo, formiranje malog CERT tima za medije unutar Agencije za sajber bezbjednost, koji bi bio specijalizovan za incidente u medijskom sektoru. Taj tim bi mogao reagovati po prijavama medija, ali i proaktivno ih obavještavati o prijetnjama (npr. ako se otkrije da se sprema kampanja DDoS napada na regionalne medije).

Treća faza bi podrazumijevala integraciju i sveobuhvatnu evaluaciju: nakon, recimo, pet godina, nezavisna evaluacija bi procijenila koliko su mediji zaista bezbjedniji – da li je smanjen broj uspješnih napada, da li mediji brže obnavljaju rad nakon incidenata, da li se povećalo povjerenje javnosti u online

informisanje, i sl. Na osnovu tih nalaza, program bi se prilagođavao novim okolnostima.

Održavanje i održivost usvojenih mjera ključno je za dugoročan efekat. Finansijska održivost mora biti planirana od početka: inicijalno, međunarodni partneri (poput Evropske unije) mogu pomoći donacijama i ekspertizom, ali dugoročno država treba preuzeti finansiranje ključnih elemenata programa. To znači da stavke poput sajber obuke novinara ili održavanja sigurnosnih sistema treba uvrstiti u godišnji budžet – bilo kroz budžet medijskih kuća (podstaknuti ih da to planiraju) ili kroz budžete ministarstava nadležnih za medije, digitalnu transformaciju i slično. Institucionalna održivost podrazumijeva da uspostavljeni mehanizmi ne budu vezani samo za trajanje jednog projekta ili mandata pojedinih funkcionera. Ukoliko se, na primjer, uspostavi "hotline" za medije, on treba da preraste u redovnu službu koja će postojati i za deset godina, možda integrisana u neku od postojećih institucija. Slično, ako mediji razviju interne politike, te politike treba redovno da se ažuriraju i ostanu na snazi i nakon promjena uredništva ili vlasništva medija.

Jedan od najvažnijih faktora održivosti je ljudski faktor i kultura bezbjednosti. Cilj je da se vremenom unutar redakcija usvoji način razmišljanja gdje se digitalna bezbjednost podrazumijeva. Da novinari automatski primjenjuju naučene mjere zaštite, da urednici planiraju bezbjednosni aspekt svakog većeg istraživačkog projekta (npr. kako čuvati prikupljene podatke, kako komunikaciju sa izvorima zaštititi od potencijalnog nadzora), te da menadžment medija kontinuirano ulaže u ovaj segment kao u dio kvaliteta poslovanja. To se može postići jedino stalnim ponavljanjem i učenjem: redakcije bi, recimo, mogle uvoditi mjesečne "bezbednosne minute" na svojim sastancima – kratke sesije gdje bi podsjetili osoblje na neku mjeru ili podijelili novo saznanje o prijetnjama. Medijske i srodne organizacije mogle bi održavati godišnje seminare ili distribuisati biltene sa novostima iz oblasti digitalne bezbjednosti specifično za medije, kako bi se znanje osvježavalo.

Takođe, od suštinskog je značaja praćenje globalnih trendova i prilagođavanje. Sajber prijetnje se stalno razvijaju – ono što je juče

bila phishing poruka, danas može biti sofisticiran "deepfake" video ili ciljano spearfishing ucjenjivačko pismo novinaru.

Održiva strategija mora biti agilna: predviđati nove tipove napada i pripremati odbrane unaprijed. To se može obezbijediti kroz međunarodnu saradnju. Crna Gora, iako mala, dio je globalne informacione mreže: povezivanje sa međunarodnim inicijativama za bezbjednost novinara (npr. kroz UNESCO programe ili saradnju sa CERT timovima drugih zemalja) osiguraće dotok najnovijih znanja i praksi.

Ukratko, model implementacije mjera treba da bude inkluzivan, fazan i prilagodljiv, a održivost se oslanja na institucionalizaciju praksi i kontinuirano jačanje kapaciteta. Iako izazovno, uspostavljanje takvog sistema jedini je način da se obezbijedi da ovaj vodič ne ostane mrtvo slovo na papiru, već da crnogorski mediji zaista postanu otporniji na sajber prijetnje, danas i ubuduće.

6.
ZAKLJUČAK

Slobodni i bezbjedni mediji temelj su demokratskog društva, a digitalna bezbjednost postala je neraskidivi dio medijskih sloboda u 21. vijeku. Crnogorski mediji su, kako pokazuju istraživanja MASE, svjesni rizika s kojima se suočavaju u sajber prostoru, ali se istovremeno bore sa ograničenim kapacitetima da te rizike prevaziđu. U proteklim godinama zabilježen je porast broja i složenosti napada na redakcije, od DDoS blokada portala do podmuklih phishing prevara i kampanja dezinformisanja. Većina tih incidenata ostala je izvan radara institucija, što je ohrabrivalo napadače i ostavljalo medije da se sami snalaze. Istovremeno, samo polovična primjena bezbjednosnih mjera unutar redakcija – prosječna ocjena sopstvene zaštićenosti ispod 3 od 5, bez ijedne najbolje ocjene – potvrđuje da su ranjivosti realne i prisutne.

No, uprkos takvoj sumornoj slici, ovo nije priča bez izlaza. Naprotiv, i mediji i društvo pokazali su da razumiju značaj problema i spremni su na promjene: sve više novinara prolazi obuke, otvaraju se razgovori o zakonskim reformama, a preporuke formulisane kroz saradnju stručnjaka i medijske zajednice pružaju jasan put naprijed. Kroz ovaj vodič identifikovani su konkretni koraci koji se mogu preduzeti da se ojača digitalna bezbjednost crnogorskih medija. Oni obuhvataju i unutrašnje promjene u redakcijama, kao što su razvoj kulture sajber higijene, usvajanje najboljih praksi i protokola i sistemske mjere na nivou države,od uspostavljanja boljih mehanizama zaštite i podrške, do izmjena zakona i jačanja institucija koje brinu o digitalnom prostoru.

Ključ uspjeha leži u sprovođenju: potrebno je da preporuke ne ostanu samo na papiru. Mediji trebaju udruženo zahtijevati njihovu

realizaciju, a državni organi ih shvatiti kao investiciju u očuvanje demokratije, a ne kao nametnut trošak. Bez bezbjednih medija, koji mogu raditi bez straha od digitalnih sabotaža ili nadzora, i sloboda izražavanja i pravo građana na istinu trpe ozbiljna ograničenja.

Optimizam uliva činjenica da je problem prepoznat i da postoje resursi koji se mogu iskoristiti iskustva drugih zemalja, finansijska i tehnička pomoć EU i međunarodnih organizacija, kao i entuzijazam lokalnih IT stručnjaka i novinara koji žele napredak. Primjena modela opisanog u ovom vodiču zahtijevaće vrijeme i posvećenost, ali benefiti će biti višestruki: otporniji mediji znače kontinuitet informisanja građana i u kriznim situacijama; znače i manje autocenzure, jer će novinari imati veći osjećaj sigurnosti dok istražuju teške teme; znače naposlijetku i odvraćanje potencijalnih napadača, koji će znati da medijski sektor više nije laka meta bez zaštite.

Sve to doprinosi jačanju ukupne otpornosti crnogorskog društva na hibridne prijetnje, jer slobodan protok provjerenih informacija najbolja je brana protiv manipulacija i destabilizacije.

U zaključku, digitalna bezbjednost medija u Crnoj Gori predstavlja izazov koji se može savladati samo zajedničkim naporima. Potrebno je istovremeno graditi znanje i svijest unutar medija, modernizovati i prilagoditi institucionalni okvir, te osnažiti vezu povjerenja između novinara, publike i institucija. Svaki novinar koji nauči kako da zaštiti svoje podatke, svaka redakcija koja usvoji novi sigurnosni protokol, svaka policijska istraga koja otkrije počinioce sajber napada – korak su bliže cilju da internet bude prostor slobode, a ne prijetnje, za medije i građane Crne Gore. Samo otporan medij je uistinu slobodan medij, a slobodan medij je čuvar javnog interesa i demokratskih vrijednosti. Upravo zato, ulaganje u digitalnu bezbjednost nije trošak, već investicija u slobodu i budućnost crnogorskog novinarstva.

7.
REFERENCE

Prilikom izrade ovog dokumenta korišćeni su i analizirani podaci sledećih institucija i organizacija:

1. Medijska asocijacija Jugoistočne Evrope (MASE).
2. Agencija za elektronske medije Crne Gore.
3. Zakon o informacionoj bezbjednosti.
4. Strategija sajber bezbjednosti Crne Gore 2022–2026.
5. Zakon o zaštiti podataka o ličnosti.
6. Ustavni sud Crne Gore.
7. Savjet Evrope.
8. Evropska komisija.
9. UNESCO.
10. Institut za medije
11. Centar za damokratsku tranziciju (CDT)