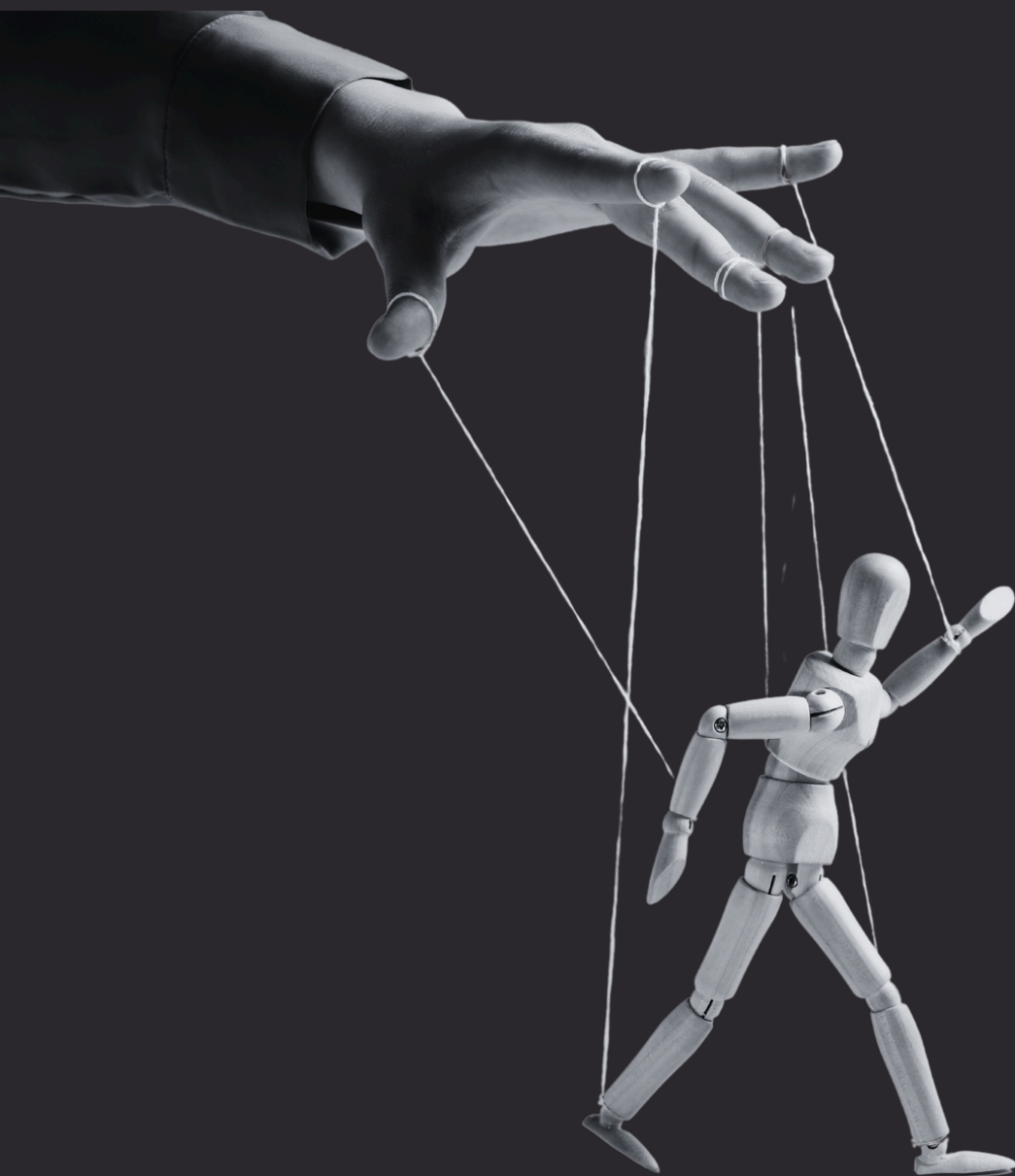


RADIKALNI BRIF

SIGURNOST NA DRUŠTVENIM MREŽAMA: KAKO SE ZAŠTITITI OD MANIPULACIJA

SNEŽANA NIKČEVIĆ



Kofinansira
Evropska unija



Ministarstvo
javne uprave



Institut za medije Crne Gore
Montenegrino Media Institute

MOD
Mreža za **Otvoreni** Dijalog



INSTITUT ZA DRUŠTVENO
POLITIČKA ISTRAŽIVANJA
— ANALITICO —



**OVU PUBLIKACIJU JE KOFINANSIRALA EVROPSKA UNIJA I
MINISTARSTVO JAVNE UPRAVE U CRNOJ GORI. NJEN SADRŽAJ
JE ISKLJUČIVA ODGOVORNOST MREŽE ZA OTVORENI DIJALOG
I INSTITUTA ZA DRUŠTVENO POLITIČKA ISTRAŽIVANJA -
ANALITICO I NE ODRAŽAVA NUŽNO STAVOVE
EVROPSKE UNIJE I MINISTARSTVA JAVNE UPRAVE.**

UVOD

Društvene mreže su postale integralni dio naše svakodnevice, nudeći nam nebrojene mogućnosti za komunikaciju, dijeljenje sadržaja i izražavanje. Međutim, uz sve prednosti, prisutnost na društvenim mrežama nosi i značajne rizike, kao što su manipulacija, zloupotreba podataka i širenje dezinformacija. Razumijevanje ovih prijetnji i usvajanje osnovnih mjera sigurnosti ključni su za našu zaštitu.

Dijeljenje fotografija, video-zapisa i ličnih misli postalo je rutina, posebno kod mladih. Ipak, postavlja se pitanje: da li smo svjesni šta se dešava s informacijama koje dijelimo? Zloupotreba ličnih podataka kao što su lokacije, životne navike i osjetljive informacije, može imati ozbiljne posljedice, uključujući krađu identiteta i narušavanje privatnosti. Na društvenim mrežama lako je stvoriti lažni identitet i manipulirati tuđim podacima.

Jednostavne lozinke, nepažljivo dijeljenje informacija ili ukazivanje povjerenja nepoznatim kontaktima često su dovoljan povod za zloupotrebu. Postoji veliki broj aplikacija koje mogu kompromitovati naše sigurnosne postavke, otkrivajući privatne podatke i pružajući pristup zlonamjernim pojedincima. Važno je razviti svijest o digitalnoj sigurnosti. Prvi korak je razumijevanje kako naše aktivnosti na mreži utiču na algoritme i šire digitalni trag. Na primjer, oglasi koje kliknemo, sadržaji koje gledamo i lokacije koje dijelimo oblikuju naše online iskustvo, ali mogu biti i iskorišćeni u svrhe koje ne kontrolisemo.

Iako tehnologija napreduje brzo, ljudski faktor ostaje najveći izazov u ovoj oblasti. Edukacija o tome kako prepoznati manipulaciju i zaštititi lične podatke ključna je ne samo za pojedince, već i za zajednice.

Uz osnovno znanje i svijest o rizicima, možemo bezbjednije koristiti društvene mreže, istovremeno čuvajući svoju privatnost i integritet.



Kako se društvene mreže zloupotrebljavaju

Bot mreže: Razmjera i efekti

Bot mreže su jedan od najčešćih alata za manipulaciju na društvenim mrežama. Ovi automatizovani profili, kreirani da imitiraju stvarne korisnike, masovno dijele dezinformacije i propagandu kako bi stvorili lažni utisak popularnosti određenih ideja ili diskreditovali protivnike.

Cilj bot mreža može biti širenje dezinformacija, stvaranje lažnog utiska o popularnosti određenih ideja ili proizvoda, pa čak i destabilizacija političkih sistema. Ove mreže mogu generisati hiljade objava dnevno, stvarajući iluziju da postoji velika podrška određenim stavovima ili idejama.

Jedan od najpoznatijih primjera zloupotrebe bot mreža bio je tokom američkih predsjedničkih izbora 2016. godine. Istraživanja su pokazala da su hiljade automatizovanih naloga širile lažne vijesti i propagandu, čime su uticale na javno mnjenje i stvorile percepciju da su određeni kandidati ili stavovi bili mnogo popularniji nego što su zaista bili. Ove aktivnosti su dovele do ozbiljnih zabrinutosti u vezi sa integritetom izbora, jer je bilo teško razlikovati stvarne glasove od manipulisanih.



Deepfake tehnologija i AI

Napredak u vještačkoj inteligenciji doveo je do razvoja deepfake tehnologije, koja omogućava kreiranje uvjerljivih lažnih video-snimaka i fotografija. Deepfake sadržaji mogu biti korišćeni za diskreditaciju javnih ličnosti, širenje lažnih informacija, pa čak i za ucjene i druge oblike prevare. S obzirom na to da je teško razlikovati stvarne od lažnih video sadržaja, ovo stvara ozbiljan izazov za prepoznavanje stvarnih izvora informacija.

Jedan od poznatih primjera deepfake tehnologije bio je u junu 2019. godine, kada je na internetu postavljen deepfake video koji prikazuje Marka Zuckerberga, osnivača Facebooka, kako izgovara riječi koje nikada nije rekao. Video je napravljen kako bi demonstrirao koliko uvjerljivi mogu biti deepfake sadržaji, a istovremeno je ukazao na rizike koji dolaze sa ovom tehnologijom.

Generativni modeli su vrsta AI modela koji su specijalizovani za generisanje novih podataka koji su slični onima koji su korišćeni tokom obuke modela. Oni imaju sposobnost stvaranja novih primjera koji nijesu nužno prisutni u originalnom skupu podataka, a cilj im je da što vjernije repliciraju osobine podataka na kojima su trenirani.

Mikrotargetiranje i sponzorisani sadržaji

Društvene mreže koriste složene algoritme kako bi personalizovale sadržaj za korisnike, ali ova tehnologija može biti zloupotrijebljena kroz mikrotargetiranje. Marketinške kompanije i političke organizacije koriste prikupljene podatke kako bi ciljano plasirale poruke specifičnim grupama ljudi, često bez njihovog znanja.

Ovo omogućava da se poruke usmjere na određene demografske grupe, utičući na njihove odluke i ponašanje. Jedan od najpoznatijih slučajeva bio je Cambridge Analytica iz 2018. godine, kada je ova firma nezakonito prikupila podatke miliona korisnika Facebooka bez njihovog pristanka. Podaci su korišćeni za mikrotargetiranje političkih oglasa, omogućavajući političkim organizacijama da ciljaju specifične grupe korisnika i utiču na njihovo informisano donošenje odluka. Ovaj događaj je izazvao globalnu diskusiju o etici u korišćenju ličnih podataka i postavio ozbiljna pitanja u vezi sa privatnošću na društvenim mrežama.

Viralni izazovi: Opasnosti na TikToku

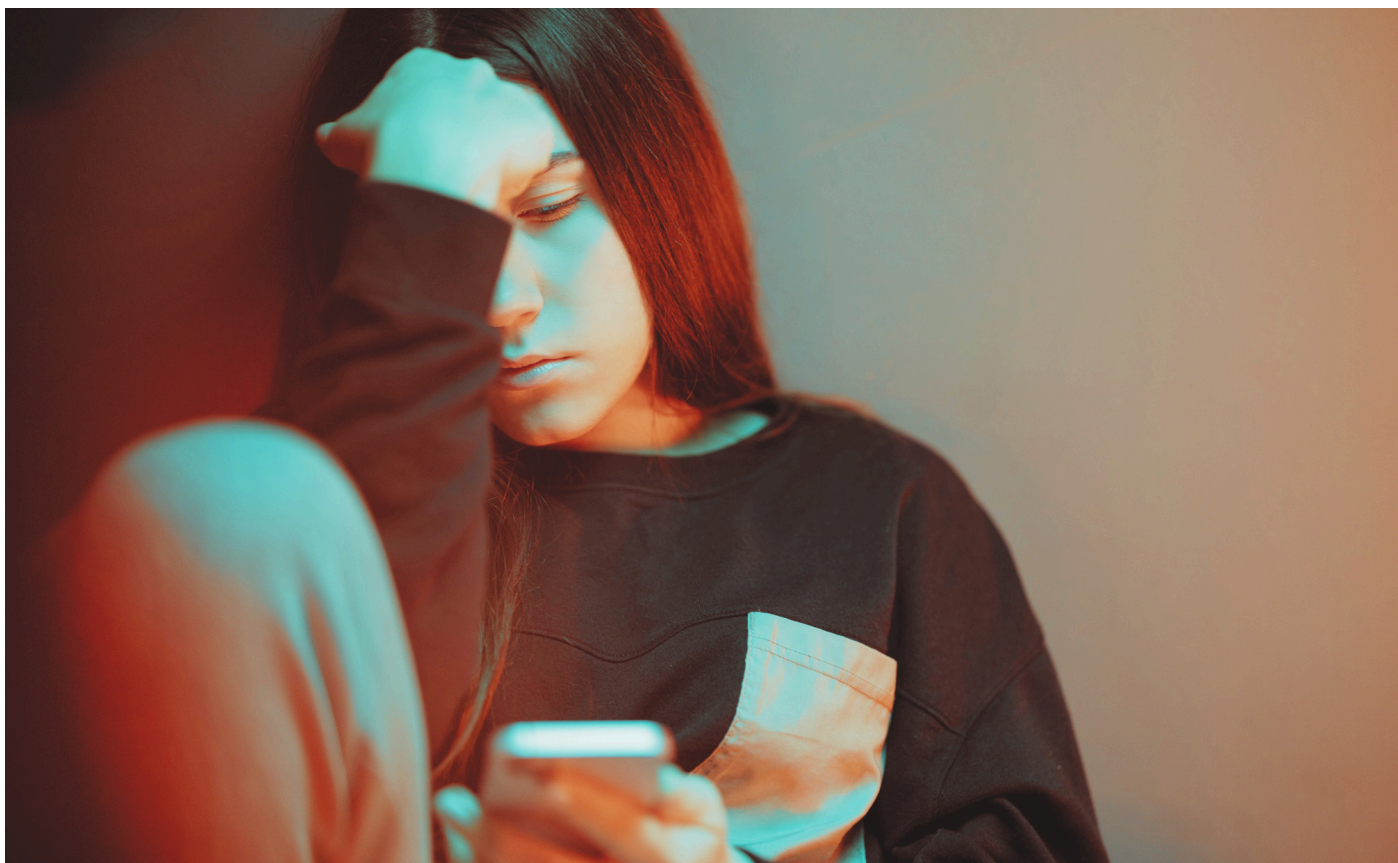
TikTok je platforma koja je postala poznata po viralnim izazovima. Ovi izazovi obično uključuju zabavne aktivnosti, ali ponekad mogu biti izuzetno opasni. Nažalost, neki od tih izazova mogu dovesti do ozbiljnih povreda pa čak i tragičnih ishoda. Posebno zabrinjavajući su izazovi koji uključuju fizičke opasnosti, kao što je izazov "Blackout Challenge", koji je postao poznat na TikToku.

"Blackout Challenge" je izazov na ovoj platformi koji je podsticao, uglavnom mlade, da se guše dok ne izgube svijest. Imajući u vidu činjenicu da je ovaj izazov rezultirao imajući nekoliko žrtava širom svijeta, skrenuo je pažnju na ozbiljne rizike koji dolaze sa viralnim izazovima na društvenim mrežama. Mladi ljudi, često motivisani željom za popularnošću, mogu nesvjesno učestvovati u opasnim aktivnostima bez razumijevanja ozbiljnosti potencijalnih posljedica.

Ovaj incident je postavio pitanje odgovornosti platformi poput TikToka, pogotovo kada govorimo o moderiranju sadržaja i edukaciji korisnika o bezbjednom ponašanju na internetu.

Ove zloupotrebe društvenih mreža ukazuju na potrebu za većim razumijevanjem medijske i digitalne pismenosti i regulacijom online prostora. Manipulacija kroz bot mreže, deepfake sadržaje, mikrotargetiranje i viralne izazove ukazuju na to koliko je važno da društvene mreže preuzmu odgovornost za sadržaj koji omogućavaju, kao i za sigurnost svojih korisnika. Regulacija, edukacija i veća svijest o opasnostima u digitalnom okruženju ključni su za zaštitu od manipulacija i štetnih uticaja u online prostoru.





Uticaj na pojedinca

Informativni mjehuri i personalizacija

Jedna od ključnih karakteristika društvenih mreža je personalizacija sadržaja. Algoritmi društvenih mreža analiziraju ponašanje korisnika — šta lajkuju, komentarišu, dijele ili pretražuju — kako bi im prikazali sadržaj koji se, prema njihovim podacima, najviše poklapa s njihovim interesima. Iako ovo može olakšati pronalaženje relevantnih informacija, isto tako dovodi do stvaranja tzv. *informativnih mjehura*.

Informativni mjehuri nastaju kada osobe, pod uticajem personalizacije sadržaja, postanu izložene samo informacijama koje potvrđuju njihove prethodne stavove i uvjerenja, dok se izostavljaju suprotstavljeni ili alternativni pogledi. Ovaj efekat izaziva značajne promjene u načinu na koji ljudi percipiraju svijet. Na primjer, politički opredijeljeni korisnici mogu se nalaziti u informativnom mjehuru u kojem samo slušaju mišljenja i vijesti koje su u skladu sa njihovim političkim uvjerenjima, dok su suprotni stavovi izloženi minimalnoj pažnji ili potpuno ignorisani.

Ovaj proces smanjuje prostor za kritičko razmišljanje, jer izostaje analiziranje različitih izvora informacija i često oni koji su u ovim mjehurima postaju potpuno uvjereni u ispravnost svojih stavova. Na duže staze, informativni mjehuri mogu dovesti do polarizacije društva, jer pojedinci postaju izolovani u svojim stavovima i sve manje su spremni da prihvate ili razmotre različite perspektive. Ovaj fenomen ima ozbiljan uticaj na međuljudske odnose i društvenu koheziju, jer povećava šanse da ljudi ne prepoznaju zajedničke tačke interesa ili da prihvate konstruktivan dijalog s onima koji imaju suprotna mišljenja.



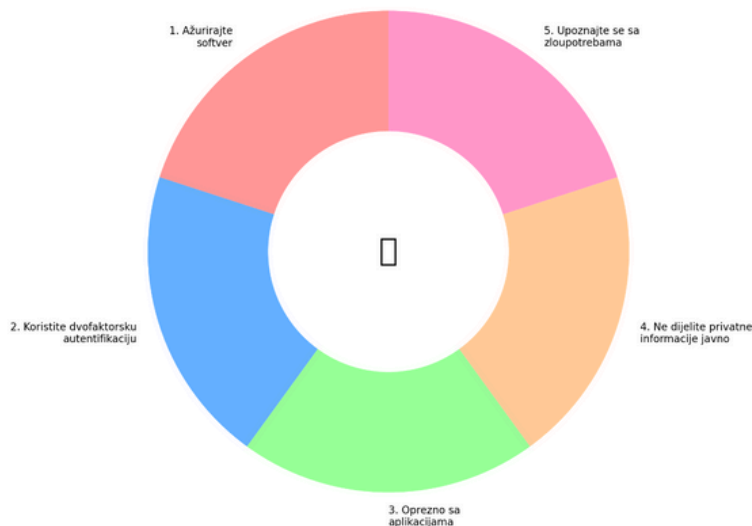
Emocionalna manipulacija

Društvene mreže takođe igraju ključnu ulogu u emocionalnoj manipulaciji korisnika. Lažne vijesti i dezinformacije često nijesu samo netačne informacije, već su dizajnirane da izazovu snažne emocionalne reakcije. Osobe koje se nalaze u *informativnim mjehurima* ili koje su podložne dezinformacijama često reaguju intenzivno jer same informacije koje im se plasiraju obično igraju na njihove najveće strahove, nade, bijes ili tugu. Primjer takve manipulacije može biti lažna vijest koja širi strah od određene bolesti, izazivajući paniku i prekomjernu reakciju.

Ovakav vid manipulacije nije ograničen samo na negativne emocije poput straha i bijesa. Često se koriste i pozitivne emocije, poput nade ili optimizma, kako bi se stvorio osjećaj euforije ili entuzijazma, što može biti iskorišćeno u marketinške ili političke svrhe. Na primjer, političke kampanje često koriste sadržaj “nabijen” emocijama kako bi stvorile osjećaj zajedništva, patriotizma, ili čak opasnosti. Na taj način oni manipulišu, ili podstiču ljude na određene akcije.

Emocionalna manipulacija ne samo da utiče na stavove, već oblikuje i svakodnevne odluke. Od političkog glasanja do odluka o kupovini proizvoda, ljudi često donose odluke koje nijesu zasnovane na racionalnoj procjeni, već na emocionalnom uticaju koji je izazvan sadržajem koji konzumiraju na društvenim mrežama.

Sigurnost na internetu



Koraci za zaštitu u digitalnom prostoru

Kako se zaštititi od dezinformacija na društvenim mrežama?

- Provjerite izvor informacije:
- Uvijek provjerite ko je autor objave ili članka.
- Pouzdani izvori uključuju zvanične medije, provjeren akademski sadržaj i informacije koje dolaze od stručnjaka u relevantnim oblastima.
- Ako je izvor anonimn ili nepoznat, budite skeptični.
- Provjerite datum objave:
- Stare informacije mogu biti predstavljene kao nove kako bi izazvale reakcije.
- Obratite pažnju na kontekst i aktuelnost objave.
- Uporedite sa drugim izvorima:
- Koristite više izvora da potvrdite tačnost informacije.
- Ako su svi kredibilni izvori dosljedni u svojim tvrdnjama, informacija je vjerovatno tačna.
- Obratite pažnju na ton i emocije:
- Dezinformacije često koriste senzacionalističke naslove ili sadržaje koji izazivaju paniku i ljutnju.
- Posebno obratite pažnju kada su u pitanju objave koje zvuče previše šokantno ili nevjerovatno.
- Provjerite činjenice:
- Koristite platforme za provjeru činjenica ukoliko su vam dostupne, ili lokalne resurse za provjeru informacija.

Kako zaštititi lične podatke na društvenim mrežama?

- Redovno ažurirajte softver i aplikacije:
- Instalirajte najnovije verzije kako biste imali pristup bezbjednosnim “zakrpama” (eng: patches).
- Koristite jake lozinke i dvofaktorsku autentifikaciju (2FA):
- Kreirajte lozinke koje kombinuju slova, brojeve i specijalne znakove.
- Aktivirajte 2FA kako biste dodatno osigurali svoje naloge.
- Budite oprezni sa aplikacijama trećih strana:
- Izbjegavajte povezivanje svog naloga na društvenim mrežama sa nepoznatim aplikacijama i redovno provjeravajte dozvole aplikacija koje koristite.
- Ograničite dijeljenje ličnih informacija:
- Nemojte javno dijeliti informacije kao što su adresa, broj telefona, datum rođenja ili lokacija, i prilagodite postavke privatnosti na svojim profilima.
- Obratite pažnju na znakove koji mogu ukazati na zloupotrebu:
- Ako primijetite sumnjive aktivnosti na svom nalogu, kao što su promijenjene postavke ili objave koje niste kreirali, odmah preduzmite akciju.

Kako prepoznati dezinformacije: Korak po korak

- **Proučite naslov.** Da li je naslov clickbait? Naslovi koji obećavaju "šokantne" informacije često služe za privlačenje pažnje.
- **Pročitajte cijeli tekst.** Nemojte donositi zaključke na osnovu naslova ili kratkog uvoda.
- **Provjerite autora.** Autor članka treba da bude jasno naveden, a njegova stručnost provjerljiva.
- **Provjerite kredibilitet sajta.** Izbjegavajte sajtove sa nejasnom politikom uređivanja sadržaja ili onima koji šire teorije zavjere.
- **Provjerite linkove i citate.** Da li su citati i linkovi u tekstu autentični i vode li do kredibilnih izvora?
- **Pitajte stručnjake.** Ako ste nesigurni, obratite se stručnjaku iz relevantne oblasti ili organizacijama specijalizovanim za provjeru činjenica.





BRIF JE DIO PROJEKTA RADIKALNO 2 KOJI JE PODRŽAN JE KROZ REGIONALNI PROGRAM „NAŠI MEDIJI: AKCIJA CIVILNOG DRUŠTVA ZA STVARANJE MEDIJSKE PISMENOSTI I AKTIVIZMA, PROTIV POLARIZACIJE I PROMOVISANJA DIJALOGA“ KOJI REALIZUJU UZ FINANSIJSKU PODRŠKU EVROPSKE UNIJE PARTNERSKE ORGANIZACIJE SEENPM, ALBANSKI MEDIJSKI INSTITUT, MEDIACENTAR SARAJEVO, VIJEĆE ZA ŠTAMPU KOSOVA , INSTITUT ZA MEDIJE CRNE GORE, MAKEDONSKI INSTITUT ZA MEDIJE, NOVOSADSKA NOVINARSKA ŠKOLA, MIROVNI INSTITUT I BIANET.

Mreža za otvoreni dijalog

JANUAR 2025. GODINE

WWW.MOD-ODN.ORG