



This work is licensed under a CC BY-NC 4.0 license  
© author(s)

Pregledni članak  
Primljeno: 2. ožujka 2023.  
<https://doi.org/10.46672/ms.23.1.4>

Ante Josip Milas\*  
Ivan Dunder\*\*

## Informacije narušenog integriteta: teorijsko određenje i ugroza nacionalne sigurnosti

### Sažetak

U suvremenom informacijskom prostoru izloženi smo mnogobrojnim informacijama među kojima su i informacije narušenog integriteta. Iako manipulacije informacijama u javnom informacijskom prostoru nisu novost, njihova količina i brzina diseminacije putem internetskih društvenih mreža i komunikacijskih operativnih sustava predstavljaju novi izazov i ugrozu za nacionalnu sigurnost demokratskih država. U javnom prostoru se koristi nekoliko različitih termina kojima se nastoji objasniti da je integritet informacije plasirane u javni prostor bitno narušen što za posljedicu ima terminološko i kognitivno nerazumijevanje. Ovaj rad istražuje i teorijski određuje vrste informacija narušenog integriteta kao što su zlonamjerna i pogrešna informacija te dezinformacija. Potom rad prikazuje primjere institucionalnog suzbijanja širenja informacija narušenog integriteta na internetu i prikazuje ugrozu koju one predstavljaju za nacionalnu sigurnost demokratskih društava.

**Ključne riječi:** informacija narušenog integriteta, zlonamjerna informacija, pogrešna informacija, dezinformacija, nacionalna sigurnost, informacijske i komunikacijske znanosti

### Uvod

Izazovi koje neistine, propaganda i dezinformacije predstavljaju za otvorena društva prepoznati su još s izumom tiskarskog stroja u 15. stoljeću, kada je prvi put u povijesti omogućeno masovno dijeljenje informacija. U kolumni objavljenj za *The Atlantic* 1919. Walter Lippmann iznio je sveobuhvatan pogled na probleme koje propaganda predstavlja za moderno zapadno društvo (prema Sproule, 1997). Lippmann (1922) je

\* Ante Josip Milas, univ. spec. pol., doktorand, Odsjek za informacijske i komunikacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu, Zagreb, Hrvatska, ajmilas@gmail.com

\*\* Doc. dr. sc. Ivan Dunder, Odsjek za informacijske i komunikacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu, Zagreb, Hrvatska, ivandunder@gmail.com

tvrdio da je temeljni izazov demokracije zaštititi vijesti kao izvor javnog mnijenja od mrlja propagande, a nijedno moderno društvo koje nema dovoljno sredstava za otkrivanje laži ne može se nazvati slobodnim. Bez potpunih, objektivnih, cjelovitih i pouzdanih informacija s integritetom, demokracijama će biti teško funkcionirati. Informacije narušenog integriteta (INI), kao što su dezinformacije i pogrešne informacije, simboli su većeg društvenog problema, a to je manipulacija javnim mnijenjem s ciljem utjecaja na stvarni svijet i ostvarenja željenih rezultata (Gu et al., 2017).

Razvoj informacijskih i komunikacijskih tehnologija utjecao je na brži protok informacija te je danas u stvarnom vremenu moguće pratiti događaje u skoro svakom kutu Zemlje. Donedavno je zamisao da svaka pozicija na Zemlji ima pristup internetu imala, između ostalih, i svoja infrastrukturna ograničenja jer je pretpostavljala razvijenu mrežu zemaljskih antena i repetitora za čije je napajanje potreban neprekidan izvor električne energije u izrazito nepristupačnim područjima na kopnu i moru. Uz to, postavljalo se pitanje ekonomske isplativosti takvih projekata. Međutim, situacija se mijenja te se postupno razvija mreža telekomunikacijskih satelita koja i u najudaljenijim dijelovima Zemlje, uz pomoć zemaljskih mobilnih prijemnika, omogućuje pristup širokopojasnom internetu.<sup>1</sup>

Danas je informacijsko-komunikacijska tehnologija, odnosno informacija, globalna pokretačka sila razvoja (Tuđman, 2012). Krajem 20. stoljeća o tome svjedoče konvencije i povelje međunarodnih organizacija te većina zakona demokratskih država koji informaciju definiraju kao razvojni potencijal koji mora biti svima dostupan. Pravo na pristup informacijama smatra se jednim od temeljnih ljudskih prava u demokratskim društvima (Tuđman, 2012). Uzrečica *tko posjeduje informaciju, ima i moć* i dalje nije opovrgnuta, iako se u doba modernih informacijskih i komunikacijskih tehnologija može govoriti i o tome da moć posjeduje onaj tko posjeduje nadzor pristupima obavijesti (Tuđman, 2008). Pojava internetskih društvenih mreža (engl. *online social media*) dodatno je ubrzala protok informacija te se danas točnost informacije vrlo često ne provjerava već se informacije (s internetskih društvenih mreža) preuzimaju u izvornom obliku i kao vjerodostojne prenose među korisnicima i u masovne medije. Posljedica takvog načina kreiranja vijesti i informiranja je pad kvalitete medijskih izvještaja i povjerenja u novinarstvo, ali i omogućavanje INI-ju zauzimanje većeg dijela javnog informacijskog prostora.

Iako manipulacije informacijama u javnom informacijskom prostoru nisu novost, njihova količina i brzina diseminacije, osobito putem internetskih društvenih mreža i komunikacijskih operativnih sustava (engl. *applications, messaging platforms*) kao što su npr. WhatsApp, Viber, Signal, Telegram i dr. predstavljaju novi izazov i ugrozu za demokraciju i njezinu sigurnost. Europska komisija u *Komunikaciji* (2018) navodi

<sup>1</sup> Jedan od trenutačno najpoznatijih je projekt *Starlink* tvrtke Space Exploration Technologies.

da se INI često koristi za podrivanje povjerenja građana u demokraciju i njezine procese. Na istome je tragu Institut Aspen (2021) objavio publikaciju *The Commission on Information Disorder Final Report* u kojoj navodi da podrivanje povjerenja građana u demokraciju označava nanošenje štete demokratskom poretku i slabljenje povjerenja građana u demokratski izabranu vlast, a narušavanje integriteta informacije je kriza kojom se pogoršavaju sve druge krize. Nadalje navode da, kada INI postane jednako učestao, uvjerljiv i postojan kao informacija s integritetom, tada uzrokuje štetnu lančanu reakciju.

Cilj je ovoga rada istražiti i odrediti različite vrste INI-ja, prikazati razlike među njima i njihove karakteristike u odnosu na informacije s integritetom te prikazati institucionalne primjere njihovog suzbijanja na internetu. U javnom prostoru često se netočno koristi nekoliko različitih pojmova kojima se vjerodostojnost objavljene informacije nastoji dovesti u pitanje. Među tim terminima posljednje desetljeće dominira termin lažna vijest (engl. *fake news*) koji se smatra sveobuhvatnim, ali nedovoljno precizno opisuje različite vrste INI-ja te je zapravo najčešće posrijedi dezinformacija ili (rjeđe) pogrešna informacija. U radu se analizom, sintezom i istraživanjem dostupne literature prikazuje teorijsko određenje i razlikovanje pojmova zlonamjerna (engl. *malinformation*) i pogrešna informacija (engl. *misinformation*) te pojma dezinformacija (engl. *disinformation*) kao različitih vrsta INI-ja. Lažne vijesti ne smatramo vrstom INI-ja već su one oblik u kojem se pojavljuju dezinformacije ili pogrešne informacije.

Prije nastavka, a zbog učestalih previda u hrvatskim publikacijama koje se bave tom tematikom i koriste terminologiju koja se odnosi na INI, smatramo da je potrebno ukratko se osvrnuti na njih. U hrvatskim stručnim i znanstvenim radovima, kao i na znanstvenim skupovima i raspravama koje proučavaju te teme, često je citirano izvješće Vijeća Europe *Information Disorder: Toward an interdisciplinary framework for research and policy making* (2017) autora Claire Wardle i Hosseina Derakhshana. Osim što doslovni prijevod engleske sintagme *information disorder* na hrvatski jezik kao „informacijski poremećaj” uvodi nepostojeći izraz u informacijskim i komunikacijskim znanostima, on je pogrešnog značenja jer pretpostavlja da je subjekt „poremećaj”, a „informacijski” opisni pridjev. Posljedično, u hrvatskom jeziku izraz ima različito i pogrešno značenje od sintagme u engleskom jeziku. Smatramo da se *information disorder* ne može doslovno prevesti jer ukoliko bi se termin kao takav prevodio na hrvatski, utoliko bi točniji, jasniji i precizniji prijevod bio „poremećaj informacija” pri čemu je gramatički ispravno i jasno da su informacije subjekt koji je poremećen. Hrvatski autorski dvojac u studiji *Jačanje otpornosti društva na dezinformacije: analiza stanja i smjernice za djelovanje* navodi da su se „u nedostatku boljih, odnosno preciznijih hrvatskih izraza, ti termini uvriježili u stručnim i znanstvenim radovima koji se bave ovom temom” (Grbeša Zenzerović i Nenadić, 2022: 10) te iz engleskog jezika doslovno preuzimaju terminologiju i koriste izraze misinformacija (od engl.

*misinformation*) i malinformacija (od engl. *malinformation*) koji u hrvatskom jeziku nemaju značenje. Osim što je potonje engleski neologizam koji nije pronašao svoje mjesto ni u engleskim rječnicima (kako se kasnije prikazuje u ovom radu), netočno je da u hrvatskoj znanstvenoj literaturi „nedostaju precizniji hrvatski izrazi” i da su se ti „termini uvriježili u stručnim i znanstvenim radovima koji se bave ovom temom” jer ih u svojim radovima upotrebljava nekolicina istih hrvatskih autora koji se bave tom tematikom. Međutim, te tvrdnje ukazuju na nedovoljno poznavanje literature iz teorije informacijske i komunikacijske znanosti i njezinih temelja u hrvatskoj znanosti. Ovaj rad argumentira te tvrdnje navodeći literaturu koja izučava predmetne teme, a koje se istražuju od zasnivanja sveučilišnog studija informacijskih i komunikacijskih znanosti u Hrvatskoj. O eventualnoj uvriježenosti izraza u stručnim i znanstvenim radovima, kao i u svakodnevnome govoru, može se govoriti samo u kontekstu termina dezinformacija. Međutim, u hrvatskoj znanstvenoj literaturi predloženi su hrvatski izrazi (npr. protuobavijest) koji nisu prihvaćeni u općoj populaciji niti su ušli u hrvatske rječnike. Stoga smatramo da se zbog nedovoljnog poznavanja terminologije informacijske i komunikacijske znanosti, u hrvatske znanstvene i stručne radove, kao i u javne rasprave koje se odnose na temu INI-ja, pogrešno uvode nepostojeći termini za vrste INI-ja koje su prethodno istražene i određene u informacijskim i komunikacijskim znanostima.

## Terminologija i teorijski temelj

U teoriji informacijskih i komunikacijskih znanosti prisutni su različiti pokušaji definiranja cjelovitosti informacije, a dosadašnji pokušaji definiranja informacije nisu ponudili jedinstvenu, općeprihvaćenu definiciju. Pregledom definicija informacije koje u trećem dopunjenom izdanju knjige *Teorija informacijske znanosti* donosi Miroslav Tuđman, može se reći da je „informacija s jedne strane neodrediv pojam iako je, s druge strane, tekstualno i dokumentarno nazočna u komunikacijskom procesu” (Tuđman, 2014: 35). Marko Sapunar u četvrtom izdanju knjige *Osnove znanosti o novinarstvu* (2004) navodi da informacija ima trajne značajke: (1) uvijek ima spoznajnu ulogu, (2) ima i ulogu aktivnog odnosa, (3) tijekom informacijskog protoka je najčešći od višeg znanja prema nižoj razini znanja i (4) informacija se uvijek transferira u ustanovljenom materijalnom obliku, kodu ili mediju jer bez toga ne bi bila perceptivna primateljima (Sapunar, 2004: 44). U novinarskom kontekstu, informacija se uglavnom shvaća kao proces prenošenja određenog znanja, tj. kao obavijest, vijest ili novost (Sapunar, 2004).

Uvriježeno mjerilo za procjenu kvalitete informacije su „točnost (objektivnost), potpunost, dostupnost i pouzdanost (engl. *currency*)” (Tuđman, 2008: 124), a integritet informacije osiguravaju jedinstvo podataka, značenja i smisla informacije. Stoga, informacija s integritetom „točno prima i percipira signale, valjano interpretira

podatke te svrhovito primjenjuje znanje u cilju rješavanja problema” (Tuđman, 2003: 59). Integritet informacije može se narušiti na trima razinama: „(a) razini integriteta podataka, (b) razini integriteta značenja i (c) razini integriteta smisla, tj. odlučivanja” (Tuđman, 2003: 59–60). Narušavanje integriteta informacije na razini integriteta podataka je pogreška u prijenosu i/ili prijmu signala, a u drugom slučaju, na razini integriteta značenja, prilikom interpretacije dolazi do pogreške da znak krivo upućuje na objekt spoznaje, ili do upućivanja znaka na krivi objekt spoznaje. Druga razina pogreške pretpostavlja prvu, a treća, u kojoj pogreškom na razini integriteta smisla dolazi do uspostave pogrešnog odnosa između obavijesti i akcije, bilo da se na temelju pogrešnih obavijesti donose pogrešne procjene problema i/ili pogrešne odluke, pretpostavlja drugu i prvu (Tuđman, 2003).

Europska komisija, tj. Stručna skupina na visokoj razini za lažne vijesti i dezinformacije na internetu (*High Level Expert Group on Fake News and Online Disinformation*, HLEG) informaciju s integritetom uspoređuje s integritetom demokratskog izbornog procesa te je određuje kao informaciju od povjerenja koja je transparentna, pouzdana i dostupna. Pri tome HLEG stavlja naglasak na građansku slobodu izražavanja i slobodu primanja i prenošenja informacija (HLEG, 2018: 12).

Za potrebe ovog rada informacija se proučava u komunikacijskom procesu te je određena kao rezultat obrade podataka, priopćenje, obavijest o činjenicama, tj. novost koju prenosi kompetentan izvor i/ili drugi medij (izvjestiteljska agencija, radio, televizija) recipijentu koji ne zna informaciju i time povećava njegov stupanj znanja. Informacija s integritetom definirana je kao pouzdan i dostupan sadržaj koji se otkriva u komunikaciji pri čemu sadrži objektivne činjenice te cjelovite, točne, potpune i relevantne iskaze o predmetu na koji se odnosi. Kako će biti prikazano u nastavku, riječ je o ključnim karakteristikama informacije kojima se manipulira ili koje izostaju kod dezinformacije te pogrešne i zlonamjerne informacije. Za analizu na teorijskoj razini, potrebno je odrediti njihova obilježja, razlike i odnose između vrsta INI-ja. Autori istraživanje započinju analizom zlonamjernih informacija kao koncepta koji se tek nedavno pojavio u informacijskim i komunikacijskim znanostima. Potom autori rada istražuju pogrešne informacije i dezinformacije nakon čega iznose primjere pokušaja njihovog suzbijanja na institucionalnoj razini te zaključak.

### ***Zlonamjerna informacija***

U hrvatskom jeziku ne postoji uvriježeni termin za englesku sintagmu *malinformation*. Pretragom poznatih engleskih mrežnih rječnika Oxford, Cambridge i Merriam-Webster autori također ne nalaze određenje tog termina.<sup>2</sup> Prethodna spoznaja upućuje

<sup>2</sup> Pretraga mrežnih stranica <https://dictionary.cambridge.org>, <https://www.oxfordlearnersdictionaries.com> i <https://www.merriam-webster.com> izvršena je 21. veljače 2023.

na to da se radi o neologizmu, složenici latinskih riječi *mal/um* (zlo, nevolja, nesreća, nezgoda) i *informatio* (informacija, obavijest, podatak, uputa, priopćenje) (Marević, 2000). U hrvatskom jeziku pojam se može prevesti kao zlobna, maliciozna, loša, štetna, pakosna ili zlonamjerna informacija. S obzirom na to, a u potrazi za hrvatskim nazivom, za pojam *malinformation* predlaže se i u radu koristi izraz zlonamjerna informacija jer blisko i jasno određuje značenje i narav pojma.

Wardle i Derakhshan (2017) zlonamjernu informaciju određuju kao destruktivnu, štetnu informaciju koja se temelji na stvarnosti, istini, izvornom dokumentu, događaju i slično, a koja se objavljuje s namjerom da uzrokuje pakost, štetu, zlobu ili ocrnjivanje objekta na kojeg se odnosi, bilo da se radi o osobi, organizaciji, državi, ideji, projektu i drugo. Zlonamjerna informacija prvenstveno ima destruktivnu namjeru i često je utemeljena na informacijama koje se nastoje držati u tajnosti i privatnosti, a do kojih se došlo na ilegalan način, narušavanjem prava na privatnost, kršenjem zakona ili oduvanjem od strane izvora koji želi nanijeti štetu. Pojavljuje se u različitim oblicima kao što su audiovizualni zapisi, ilustracije, tekst, privatna e-pošta, tekstualne poruke i dr. (Wardle i Derakhshan, 2017). Wardle (2019b) dodaje da je karakteristika zlonamjerne informacije i namjerna manipulacija kontekstom, datumom ili vremenom nastanka izvornog sadržaja. Namjerna manipulacija informacijom upućuje nas na to da je zlonamjerna (manipulirana) informacija ustvari dezinformacija jer sadrži karakteristike dezinformacije koje autori prikazuju u nastavku rada. Osim manipulacije, integritet zlonamjernih informacija osporava se zbog njezine svrhe i namjere da uzrokuje štetu, ali i zbog ilegalnog načina prikupljanja koji dovodi u pitanje vjerodostojnost informacije. Međutim, što kada zlonamjerna informacija sadrži točne, potpune, cjelovite iskaze i nepristrane podatke te time posjeduje karakteristike informacije s integritetom? To se rijetko događa jer, s obzirom na štetnu namjeru, često je slučaj da autor zlonamjerne informacije svjesno izostavlja dio (ili više njih) informacije ili kontekst koji bi mogao ići u prilog objektu kojem se nanosi šteta ili bi mogao štetiti autoru zlonamjerne informacije.

U kontekstu političke komunikacije i odnosa s javnošću, Siniša Kovačić (2021) zlonamjerne informacije spominje kao curenje informacija koje dijeli na kontrolirano i nekontrolirano. Kontrolirano curenje informacija može biti učinkovit način priopćavanja onoga što vlada smatra da je informacija visokog potencijala za, primjerice, odvratanje pozornosti javnosti, dok se nekontrolirano curenje smatra znakom dobrog novinarstva (Kovačić, 2021). Posljednjih desetljeća su, posebno u politici, poznate velike afere objave podataka prikupljenih kontroliranim ili nekontroliranim curenjem, a za koje je u trenutku publiciranja postojala dilema o javnom interesu ili isključivoj namjeri nanošenja štete njihovom objavom. Među njima možemo navesti afere danas poznate pod nazivima *Pentagon Papers*, *Wikileaks*, *Watergate* i dr. Uz to, u recentnoj literaturi koja proučava zlonamjerne informacije često se kao primjer zlonamjernih

informacija navodi javna objava privatne e-pošte kandidatkinje za predsjednicu Sjedinjenih Američkih Država (SAD) Hillary Clinton tijekom izborne kampanje 2016. (Allcott i Gentzkow, 2017).

U javnosti su učestalo prisutni primjeri objava privatne korespondencije javnih osoba, uglednika i institucija koje su prikupljene ilegalnim prodorom u sustav ili drugim ilegalnim načinima, a čija je namjera nanošenje štete. I u Hrvatskoj postoje primjeri objave takvih informacija. Kao primjer može se spomenuti članak u tjedniku Nacional u kojem je objavljena navodna korespondencija pripadnika sigurnosno-obavještajne agencije koja se odvijala na komunikacijskom operativnom sustavu WhatsApp (Nacional, 2019). Kako se navodi, „poruke s WhatsAppa koje je Nacionalu ustupio izvor iz Vojne sigurnosno-obavještajne službe predstavljaju materijalne tragove za koje se tvrdi da otkrivaju da je VSOA provela špijunsku operaciju izvan svojih ovlasti” (Nacional, 2019). Autentičnost poruka nije potvrđena niti su prezentirani dodatni dokazi tvrdnji u članku, ali je implikacijom da se postupa izvan zakonskih okvira učinjena šteta sigurnosno-obavještajnom sustavu Republike Hrvatske. Kao sljedeći primjer mogu se navesti javne objave klasificiranih dokumenata, kao što su npr. policijski spisi i dokazni materijali u sudskim procesima, a koje su učestale u hrvatskim medijima. U svibnju 2020. Ured za suzbijanje korupcije i organiziranog kriminaliteta (USKOK) je u tzv. aferi *Vjetroelektrane* donio rješenje o provođenju istrage protiv 13 poduzetnika i državnih dužnosnika, među kojima je bila i državna tajnica. Nakon pokretanja istrage u medijima je objavljen sadržaj provedenih dokaznih radnji, a kao izvor curenja podataka spominjali su se USKOK i Državno odvjetništvo Republike Hrvatske (DORH) što je ubrzo iz DORH-a i USKOK-a demantirano (DORH, 2020). Međutim, šteta je učinjena i rad DORH-a i USKOK-a je diskreditiran. Taj primjer pokazuje da se objavom sadržaja provedenih dokaznih radnji nastojala nanijeti šteta ugledu državnih institucija, koje su ujedno sastavnica sustava nacionalne sigurnosti te moguće osujetiti provođenje kaznenog postupka protiv osumnjičenih osoba.

U želji za ostvarivanjem većeg profita i maksimiziranjem dobiti, mnogi poslovni i privatni subjekti svojim objavama na mrežnim stranicama nastoje privući korisnike da kliknu na sadržaj koji su objavili kako bi povećali broj pretplatnika ili broj dijeljenja svojih objava. Time povećavaju svoju vidljivost i doseg, što u konačnici donosi mogućnost ostvarivanja većeg profita. Često su upravo zlonamjerne informacije mamilice koje privlače veći broj klikova (engl. *clickbait*), a koje donose veću financijsku korist na štetu privatnosti onih na koje se informacija odnosi.

O zlonamjernim informacijama kao o „zlu koje je prikriveno u komunikaciji koja ne izgrađuje zajedništvo” govorio je i papa Franjo povodom 52. svjetskog dana sredstava društvene komunikacije. Poručio je: „besprijekorni argument može se, naime, temeljiti na neospornim činjenicama, ali ako se koristi zato da se povrijedi drugoga i da se tu osobu diskreditira u očima drugih, koliko god izgledao ispravno, nije istinit.



Istinitu izjavu možemo prepoznati po njezinim plodovima: potiče li svađu, raspiruje li podjele, širi li resignaciju, ili, pak, promiče informirano i zrelo promišljanje koje vodi prema konstruktivnom dijalogu i plodonosnim rezultatima” (Papa Franjo, 2018).

Sadržaj Papine poruke može navesti na zaključak da su, bez obzira na to što se temelje na činjenicama, zlonamjerne informacije doista vrsta INI-ja upravo zbog svojih karakteristika kao što su zla namjera da se ošteti drugoga, da se diskreditira druga osoba, kao i zbog negativnih posljedica koje donose.

U novinarstvu postoje etičke dileme o tome je li objava prikupljenih informacija u javnom interesu ili je posrijedi namjera nanošenja štete. Štetnu namjeru je izazovno dokazati te je iz tog aspekta koncept zlonamjernih informacija diskutabilan kada se razmatra jesu li zlonamjerne informacije vrsta INI-ja ili jedan od oblika dezinformacije. Stoga, autori ovoga rada smatraju da je o zlonamjernim informacijama potrebno provesti dodatna istraživanja i rasprave u koje će biti uključeni teoretičari, znanstvenici i stručnjaci iz različitih područja, od informacijskih i komunikacijskih znanosti, novinarstva, filozofije, etike i drugo, kako bi se karakter i postojanje zlonamjernih informacija ispravno i precizno odredio. Raspravu i istraživanje u ovome članku autori smatraju doprinosom u tom smjeru i nastojanjem da se otvore nova pitanja za promišljanje o biti zlonamjernih informacija.

### ***Pogrešna informacija***

Za razliku od zlonamjernih, pogrešne informacije (engl. *misinformation*) poznat su termin u teoriji informacijskih znanosti. Tuđman (2003) pogrešnu informaciju određuje kao nazoviobavijest, navodeći da ne mora nužno nastati s namjerom da zavede korisnika. Predlaže da bi se u hrvatskom jeziku kao sinonimi mogli koristiti pseudoobavijest ili kvaziobavijest, a izraz može označavati netočnu, pogrešnu, iskrivljenu obavijest. U ovome radu odlučili smo koristiti termin pogrešna informacija jer ta vrsta INI-ja nastaje kao posljedica pogreške te smatramo da taj termin jasno opisuje narav njezinog sadržaja koji prenosi netočne ili nedovoljno točne informacije. Prema Tuđmanu (2003), Tarcza i Buker za pogrešne informacije kažu da unose zbrku i nered jer su netočne, u suprotnosti s prethodnim obavijestima ili su izmijenjene u komunikacijskom procesu. Sadrže pogreške te zastarjele i subjektivne informacije, ali nisu nužno namjerni pokušaj uvjeravanja u netočnosti jer iskazuju poglede koji mogu biti krajnje subjektivni (Tarcza i Buker, 2001, prilagođeno prema Tuđman, 2003: 54–55).

Uporabom kriterija točnosti i štetnosti, Wardle i Derakhshan (2017) pogrešne informacije određuju kao informacije koje su netočne, ali nisu stvorene s namjerom nanošenja štete. Prema tome se može zaključiti da su pogrešne informacije suprotnost zlonamjernim informacijama jer, za razliku od njih, prenose netočne informacije bez namjere nanošenja štete. One nastaju kao posljedica pogrešnog izvještaja



ili izvještavanja kojem uzrok može biti nerazumijevanje ili neznanje o predmetu izvještavanja i kao takve su učestale kod novinara i u medijskom prostoru. Pogrešne informacije mogu nanijeti štetu ali, za razliku od zlonamjerne informacije, u njihovom nastanku ne postoji namjera činjenja štete. Wardle (2019b) dodatno proširuje prethodnu definiciju te kaže da je jedna od mogućnosti nastanka pogrešnih informacija kada se satirične vijesti shvate ozbiljno ili kada dođe do pogreške u prijevodu, interpretaciji statističkih podataka, naslova i datuma.

HLEG (2018: 10) pogrešne informacije sažeto određuje kao zavaravajuće ili netočne informacije koje dijele osobe koje ih ne prepoznaju kao takve, a odgovornost za širenje pogrešnih informacija stavlja na pojedinca i osobnu medijsku pismenost. Jack (2017) pogrešne informacije definira kao informacije čija je netočnost nena-mjerna, uključujući novosti objavljene pogreškom, a koje se mogu proširiti kada ih novinari pogrešno protumače ili propuste neovisno provjeriti tvrdnje izvora radi brzog objavljivanja informacija, bilo zbog aktualne krize ili konkurencije.

Primjeri pogrešnih informacija učestali su kod prevođenja te pogrešaka u prijevodu sa stranog jezika što rezultira pogrešnom informacijom. Osim u medijima, takve primjere pogrešnih informacija često nalazimo na kulturnim spomenicima, muzejima, privatnim ili javnim obavijestima. Poznati primjer javne obavijesti s pogrešnim informacijama dogodio se za vrijeme koronakrize kada je Hrvatski zavod za javno zdravstvo (HZJZ) objavio upute na hrvatskom i engleskom jeziku. Osim pravopisnih grešaka, uputa koja je glasila „izbjegavajte rukovanje...” na engleski je jezik prevedena kao „avoid handling...” umjesto „avoid handshakes” što kod čitatelja koji ne zna hrvatski može izazvati zbunjenost, nerazumijevanje i navesti na krivo postupanje. Iako je taj primjer benigni i ne dočarava sve opasnosti pogrešne informacije, postoje i mnogi drugi primjeri pogrešaka u prijevodu koji osim nesporazuma imaju ozbiljnije posljedice na zdravlje, financije, pravosuđe, sigurnost i ljudske živote.

Kao što navodi Jack (2017), pogrešne informacije mogu se proširiti zbog nedostatka kvalitetnog rada novinara. Kvaliteta novinarskih izvještaja i prenesenih informacija gubi u odnosu na brzinu i potrebu biti prvi, biti prije konkurencije te novinari stoga često ne provjeravaju točnost informacije prije objave. Tako su u rujnu 2020. vijesti HRT-a na Twitteru (@hrtvijesti) objavile kako je u tzv. aferi Janaf između ostalih uhićen javnosti poznat političar i zastupnik u Gradskoj skupštini Grada Zagreba, a ustvari se radilo o uhićenju druge osobe istog prezimena (Jutarnji list, 2020). Na objavljenu pogrešnu vijest na Twitteru osobno je reagirao prozvani zastupnik objavivši da nije uhićen niti osumnjičen te da je došlo do pogreške novinara HRT-a. Takva objava s netočnim podacima zasigurno je nanijela štetu ugledu krivo imenovane osobe. Kada se na pogrešne informacije ne reagira dovoljno brzo i na adekvatan način (neophodnim demantijem i isprikom), one mogu trajno ostati

zabilježene u kolektivnoj memoriji i utjecati na proces odlučivanja. Popravlak nastale štete u internetsko doba izrazito je zahtjevan i izrazito težak posao. Pogrešne informacije u novinarstvu su učestale, a posljedice ponekad uključuju podizanje sudskih tužbi za klevetu protiv novinara i novinskih redakcija.<sup>3</sup> Uz nedovoljnu informiranost i znanje izvjestitelja, u doba internetskih društvenih mreža i internetskih medija, kvaliteta izvještaja i prenesenih informacija gubi u odnosu na brzinu, a posljedica su pogrešne informacije i pad kvalitete novinarskih izvještaja.

Ne tako davno, krajem 20. stoljeća, televizija je dominirala medijskim prostorom. Televizijska mreža CNN (*The Cable News Network*) sa svojim izvjestiteljima diljem svijeta bila je bez konkurencije u prijenosu informacija i aktualnih događaja uživo. To se posebno očitovalo tijekom vojne operacije Pustinjska oluja kada su televizijski izvjestitelji CNN-a u stvarnom vremenu prenosili događaje na bojištu bez postojanja konkurencije u objavi informacija. Pojavom internetskih medija, informativnih (engl. *news*) portala i internetskih društvenih mreža, poput Facebooka i Twittera, došlo je do promjene. Pojavilo se tzv. građansko novinarstvo (engl. *citizen journalism*) i svatko s pristupom internetu i kamerom može biti izvjestitelj i prenositi informacije o događajima u tijeku, a televizija je izgubila primat. Takav novi oblik novinarstva vrlo je podložan pogrešnim interpretacijama događaja i prijenosu pogrešnih informacija, kao i dezinformacija.

Prethodno smo prikazali suprotnost između zlonamjernih i pogrešnih informacija koje su određene kao netočne informacije bez namjere nanošenja štete. Prije nastavka u kojem istražujemo i određujemo dezinformacije, potrebno je naglasiti razliku u namjeri između pogrešnih informacija i dezinformacija. Kako bi se pokazala kompleksnost određenja, razlikovanja i razumijevanja pogrešnih informacija u odnosu na dezinformacije, Wardle (2019b) navodi da se dezinformacije širenjem i dijeljenjem često pretvaraju u pogrešne informacije. Primjerice, o pogrešnoj informaciji se radi kada osoba vidi dezinformaciju za koju vrlo često vjeruje da je točna te je potom podijeli s prijateljima vjerujući da time pomaže informirati druge osobe. S druge strane, ako osoba namjerno širi netočne informacije, to je dezinformacija. Wardle (2019b) taj fenomen pojašnjava društveno-psihološkim čimbenicima i željom pojedinca za „povezivanjem s plemenom,” pripadanjem određenoj vjeri, rasi, etničkoj skupini ili drugoj interesnoj skupini. Za razliku od pogrešnih informacija, dezinformacije se stvaraju i šire s namjerom da se druge dovede u zabludu i da se načini šteta. U nastavku rada dodatno analiziramo taj oblik INI-ja koji je znatna ugroza za nacionalnu sigurnost demokratskih društava.

<sup>3</sup> Međutim, tužbama za klevetu protiv novinara nastoji se i zastrašiti i ušutkati novinare te nametnuti cenzura, što je poznato i kao SLAPP tužbe (*Strategic Lawsuits Against Public Participation*).

## *Dezinformacija*

Kako je prethodno navedeno, dezinformacija se od pogrešne informacije razlikuje u namjeri (Wardle i Derakhshan, 2017). Tuđman (2012) navodi da je pogrešna informacija nenamjerna neistinita informacija, a dezinformacija namjerna neistinita informacija, dok Wardle i Derakhshan (2017) dezinformaciju određuju kao netočnu i svjesno kreiranu informaciju objavljenu s namjerom uzrokovanja štete osobi, društvenoj skupini, organizaciji ili državi. Dezinformacija sadrži karakteristike zlonamjerne informacije (namjeru nanošenja štete) i pogrešne informacije (obmanjujući i netočan sadržaj). Razlikuju se po tome što pogrešna informacija obično implicira pogrešku i izostanak štetne namjere dok dezinformacija podrazumijeva svjesnu obmanu, zabluđu i štetnu namjeru. Međutim, namjeru je često teško dokazati te se stoga u javnom diskursu termin pogrešna informacija koristi češće od dezinformacije, a to je sklonost koju kreatori dezinformacija mogu iskoristiti i koriste kako bi pokušali održati vjerodostojnost i prikriti svoje djelovanje (Jack, 2017).

U hrvatskom rječniku dezinformacija je određena kao „namjerno kriva informacija sa svrhom da onaj koji je daje napakosti onomu o kojem je daje; zavođenje u bludnju, obmana” (Klaić, 2012), dok je u engleskom određena kao „netočna informacija koja se namjerno i često prikriveno širi (kao podmetanjem glasina) s namjerom utjecaja na javno mnijenje ili prikrivanja istine” (Merriam-Webster Dictionary, 2022). Tuđman (2003: 53) za hrvatski jezik predlaže termin protuobavijest, a kao sinonime navodi dezinformaciju, kontrainformaciju, kontraobavijest i antiinformaciju. Kao što je spomenuto, zbog učestalosti korištenja i prihvaćenosti u javnosti, u ovome radu koristi se termin dezinformacija koji je prepoznat i u Hrvatskoj enciklopediji Leksikografskog zavoda Miroslav Krleža (Hrvatska enciklopedija, mrežno izdanje, 2021). Kada se o dezinformaciji govori u kontekstu obavještajne zajednice, Watson (1990, prema Tuđman, 2003) navodi da se termin „koristi u tajnim i prikrivenim izvještajnim operacijama da opiše krivotvoreni, lažni dokaz koji se koristi za diskreditiranje protivnika.”

Dezinformacija nastaje namjernom pogreškom u komunikaciji kada izostaje jedan od uvjeta informacije s integritetom koju „određuju jezik razmjene, potpunost, objektivnost, dostupnost i pouzdanost obavijesti” (Tuđman, 2012: 97). Temelj na kojem nastaje dezinformacija je nepotpunost informacije s točnim, ali necjelovitim sadržajem. Spomenuto je i da se u recentnoj literaturi taj oblik dezinformacije naziva i zlonamjernom informacijom. Dezinformacije nastaju u „manipulaciji s (a) izvorom obavijesti, izvor obavijesti je nepoznat, (b) autorom obavijesti, nepoznat je pravi autor obavijesti i (c) pošiljateljem obavijesti, kada komunikacija s pošiljateljem nije moguća” (Tuđman, 2003: 61). Kada je obavijest namjerno nepotpuno prikazana, onda je ona dezinformacija, bez obzira na djelomičnu objektivnost i točnost (Tuđman, 2008: 125).

Kako bi se otklonila dilema i kako bi bilo moguće jasno razlikovati pogrešne informacije od dezinformacije, treba istražiti namjeru (koja se apostrofira i u prethodnoj tvrdnji) jer namjera je ključna u detekciji dezinformacije, ali izazovna za dokazivanje. Gordan Akrap (2009) dezinformaciju pri izradi izvješnica opisuje kao šum koji uzrokuje smetnje i ponaša se kao računalni virus. Smetnje u sustav mogu ući u nekom od oblika vanjskih ulaznih vrijednosti (podatak, informacija, znanje) ili kao posljedica (a) prihvaćanja krive/nametnute percepcije, (b) neispravne provjere i pregleda ulaznih podataka, (c) pogreške u tumačenju i utvrđivanju pouzdanosti te (d) pogrešnog planiranja i upravljanja (Akrap, 2009).

Dezinformacije se proizvode s namjerom da protivnika navedu na promjenu mišljenja te donošenje odluka i prosudbi na vlastitu štetu (Tuđman, 2008). Potonje je posebno izraženo u ratnim sukobima kada se protivnika nastoji navesti na donošenje krive odluke, ili nedonošenje odluke, kako bi se ostvarili vojni i politički ciljevi. Također, dezinformacijama se želi diskreditirati protivnikove ciljeve i namjere te njegov kredibilitet i vjerodostojnost kako bi se gubitkom potpore vlastite javnosti i institucija protivnika opstruiralo u provedbi njegovih planova (Tuđman, 2012). Cilj je preuzeti kontrolu nad društvenim institucijama i protivniku nametnuti vlastitu interpretaciju stvarnosti. S druge strane, dezinformacija može biti namijenjena vlastitoj javnosti za potporu ciljevima koje javnost ne bi prihvatila kada bi znala istinu (Tuđman, 2012). U tom slučaju može se govoriti o manipulacijama javnim mnijenjem koje kratkoročno mogu polučiti željeni rezultat, ali dugoročno se manipulacijama gubi kredibilitet i povjerenje u demokratske procese.

Prilagodбом postavke koja je u sociološkoj literaturi poznata kao Thomasov teorem,<sup>4</sup> profesor Tuđman je artikulirao teorem o istinitosti dezinformacije koji glasi: „ako javnost (korisnik) prima dezinformaciju kao istinitu, onda je dezinformacija istinita po svojim posljedicama” (Tuđman, 2012: 142).

Dezinformacija je dio osobnog ili javnog znanja zato što ljudi vjeruju da je istinita, a ne zato što postoje argumenti i činjenice koje bi potvrdile istinitost dezinformacije (Tuđman, 2012). Iz toga je razvidna značajna opasnost dezinformacije kada se ona u demokratskim društvima percipira i prihvati kao vjerodostojna informacija, informacija s integritetom, jer je nakon toga vrlo izazovno javnost uvjeriti da je zapravo posrijedi INI koji ima namjeru narušiti povjerenje u demokratske procese i posljedično može ugroziti nacionalnu sigurnost.

U svom izvješću HLEG (2018: 10) dezinformaciju definira kao lažnu, netočnu, obmanjujuću informaciju osmišljenu, predstavljenu i promoviranu da namjerno uzrokuje javnu štetu ili financijsku dobit. Rizik od nanošenja štete odnosi se na prijetnje de-

<sup>4</sup> Thomasov teorem: ako ljudi definiraju situacije kao stvarne, onda su one stvarne po svojim posljedicama.

mokratskim političkim procesima i vrijednostima koje mogu posebno ciljati različite sektore, poput zdravstva, znanosti, obrazovanja, pravosuđa, obrane, financija i druge. Pokreće ga proizvodnja i propagiranje dezinformacija radi ekonomske dobiti, političkih ili ideoloških ciljeva, a može se pogoršati ovisno o tome na koji način različite publike i zajednice primaju i šire dezinformacije.

HLEG (2018) smatra da je problem dezinformacija povezan sa širim političkim, društvenim, građanskim i medijskim pitanjima u Europi, nastalima prije razdoblja digitalnih medija te uključuje četiri ishodišta: (1) dezinformacije koje prenose politički dionici, (2) mediji koji zbog nedostatne profesionalnosti i nedostatne neovisnosti uredništva pridonose ekspanziji dezinformacija, (3) građani koji individualno ili kolektivno potiču dezinformacije dijeleći lažne i zavaravajuće sadržaje, a visoko polarizirana društva s niskom razinom povjerenja su plodno tlo za proizvodnju i dijeljenje ideološki motiviranih dezinformacija te (4) digitalni mediji, posebno velike internetske platforme sa sjedištem u SAD-u koje nude korisne i popularne proizvode i usluge za pretraživanje, društveno umrežavanje, slanje poruka i slično.

Martin Moore, ravnatelj Središta za proučavanje medija, komunikacija i moći na King's Collegeu u Londonu, u svome podnesku britanskom parlamentu velik dio odgovornosti za širenje dezinformacija usmjerava na velike internetske tvrtke. Smatra da „naše razumijevanje trenutnog fenomena ... ozbiljno ograničavaju same tehnološke platforme. Podatci koji bi pomogli u razumijevanju prirode i opsega problema te njegovih učinaka, zaštićeno su vlasništvo tvrtke. Sve dok platforme ne učine ove podatke dostupnima za neovisno istraživanje, bit će nemoguće u potpunosti procijeniti problem” (Moore, 2017: 8).

Istražujući utjecaj dezinformacija na demokraciju, Lance Bennett i Steven Livingston navode da „u usporedbi s erom masovnih medija, sadašnje doba prikazuje kaleidoskopski medijski krajolik koji se sastoji od televizijskih mreža, novina i časopisa (internetskih i tiskanih izdanja), sadržaja objavljenog na YouTube, WikiLeaksu i LiveLeaku, Astroturfu, radikalnih internetskih stranica koje šire dezinformacije u obliku novinarskih formata, Twittera i Facebooka (među ostalim internetskim društvenim mrežama), tvornicama trolova, botovima i temama za raspravu na 4chanu” (Bennett i Livingston 2018: 129). Također, za širenje dezinformacija važnima smatraju i druge komunikacijske kanale koji su zbog nedostupnosti podataka gotovo nemogući za proučavanje, a to su Snapchat, internetske stranice zaštićene TOR-om te komunikacijski operativni sustavi za razmjenu poruka kao što su WhatsApp, Signal, Telegram, Proton Mail i internetska telefonija (*Voice-over-Internet Protocol*).

U odnosu na prijašnje razdoblje kada je postojao manji broj komunikacijskih kanala kroz koje su se objavljivale službene informacije, a zbog promjena u medijskom sustavu kao što su razvoj medija i internetskih medijskih platformi, kontrola propusnosti informacija u masovne medije postala je vrlo izazovan zadatak. Pod utjecajem

rastućeg trenda objava dezinformacija na Facebooku i javnih prozivki zbog odgovornosti za njihovu diseminaciju, tvrtka Facebook (danas Meta, op.a.) objavila je 2017. publikaciju *Information Operations and Facebook* u kojoj dezinformaciju određuje kao: „netočna ili manipulirana informacija/sadržaj koja se namjerno objavljuje. Može uključivati pseudovijesti (engl. *false news*) ili suptilnije metode kao što su lažna upozorenja, objava netočnih citata ili laži koje su upućene nedužnim korisnicima ili svjesno širenje obmanjujućih ili pogrešnih informacija. Dezinformacija se razlikuje od pogrešne informacije koja je nehotično ili nenamjerno širenje netočnih informacija bez zle namjere” (Weedon et al., 2017: 5).

Kao i mnoge tvrtke koje posluju u medijima i nenamjerno služe kao platforma za širenje dezinformacija, tako se i tvrtka Meta suočava s izazovnim odlukama o uklanjanju dezinformacija iz širokog spektra političkih diskursa pri čemu mora balansirati između slobode govora, odnosa s korisnicima i svojim poslovnim modelom, tj. poslovnim profitom i dobiti (prilagođeno prema Bennett i Livingston, 2018). Informacijsko doba u ovom trenutku je vrlo pogodno za diseminaciju dezinformacija kao oružja za ostvarivanje interesa što je posebno izraženo u sukobima niskog intenziteta koji se odvijaju u informacijskom prostoru, ali i interpersonalnih sukoba na razini pojedinaca, konkurentskih tvrtki, političkih stranaka i drugih organizacija. Sukobi visokog intenziteta nastoje se izbjeći, a „oružane snage i obavještajne službe velikog broja država imaju pravilnike i programe dezinformiranja” (Tuđman, 2003: 69) te se stoga međunarodni sukobi niskog intenziteta odvijaju u medijskom prostoru.

## **Suzbijanje informacija narušenog integriteta i ugroza nacionalne sigurnosti**

Problematika suzbijanja INI-ja vrlo je složena i posebno osjetljiva u demokratskim društvima, prvenstveno zbog temeljnih demokratskih načela slobode misli, slobode izražavanja, slobode tiska i slobode govora. Iako postoje mnogi institucionalni pokušaji, za sada nije pronađeno jednostavno, jedinstveno i učinkovito rješenje koje bi omogućilo dijeljenje i suzbijanje INI-ja na internetu, prvenstveno dezinformacija, a koje bi bilo u skladu s demokratskim slobodama i pravima građana. Nedemokratska društva, koja institucionalno nadziru i kontroliraju medije te provode cenzuru (i druge metode) uskraćujući temeljna ljudska prava svojim građanima, mnogo jednostavnije se suprotstavljaju izazovima koje za sigurnost njihovih društava predstavlja INI.

Od prethodno navedenih i analiziranih vrsta INI-ja, dezinformacije su najveća opasnost za demokratska društva i njihovu nacionalnu sigurnost. Pojedine države članice Organizacije Sjevernoatlantskog sporazuma (NATO) i Europske unije (EU) kao što su Njemačka, Češka i Francuska, uočile su opasnosti dezinformacija za njihovo društvo i poduzele mjere za njihovo razotkrivanje i suzbijanje. Primjerice, njemačko

Ministarstvo unutarnjih poslova predložilo je osnivanje Središta za obranu od dezinformacija, a Češka je 2017. najavila osnivanje Središta za borbu protiv terorizma i hibridnih prijetnji kojem će zadaća, između ostaloga, biti borba protiv dezinformacija. U Francuskoj su se u borbu protiv dezinformacija uključili ugledni mediji kao što su *L'Express* i *Le Monde* koji u suradnji s tvrtkama Meta i Google rade na javnom razotkrivanju dezinformacija (*Cordy Report*, 2017). NATO-ov Odbor za civilnu dimenziju sigurnosti (engl. *Comitee on the Civil Dimension of Security*) državama je članicama 2017. predložio „stvaranje zasebne vladine jedinice koja će, u suradnji s internetskim društvenim mrežama, besprekidno nadgledati štetno korištenje internetskih društvenih mreža, razotkrivati lažne vijesti i neprijateljsku propagandu te im se suprotstavljati činjenicama” (*Cordy Report*, 2017: 16), između ostalog i korištenjem neklasificiranih izvjesnica, tj. obavještajnih proizvoda kao što su primjerice satelitske snimke.

U Republici Hrvatskoj dezinformacije su posebno bile aktualne i opasne tijekom Domovinskog rata i u razdoblju demokratskih promjena koje su prethodile osamostaljenju Republike Hrvatske, a čiju je samostalnost svim raspoloživim sredstvima nastojala onemogućiti Jugoslavija (ili ono što je od nje ostalo na čelu sa srbijanskom vodstvom). U provođenju dezinformacijskih kampanja u tom razdoblju osobito aktivna bila je Kontraobavještajna služba (KOS), protuobavještajna agencija tzv. Jugoslavenske narodne armije koja je izrađivala i u javni prostor plasirala dezinformacije kojima je nastojala kompromitirati hrvatsko vrhovništvo i osujetiti napore za osamostaljenje i neovisnost Hrvatske (Domović, 2010).

Danas u Hrvatskoj, kao i u drugim državama članicama EU-a i NATO-a, većina dezinformacija dolazi izvana i usmjerene su protiv demokratskog poretka s ciljem narušavanja povjerenja javnosti u demokratske procese, državne institucije, EU i NATO. One predstavljaju potencijalnu opasnost za nacionalnu sigurnost i društvenu koheziju (HLEG, 2018). Primjerice, u Ruskoj Federaciji postoje tvrtke specijalizirane za proizvodnju dezinformacija na internetskim društvenim mrežama te državnim novcem financirane medijske organizacije čija je svrha i zadaća kontinuirano i sustavno objavljivanje sadržaja koji su u skladu s ruskim nacionalnim interesima (*Cordy Report*, 2017; Shmatenko, 2019).

Osim organizacija civilnog društva, u Hrvatskoj za sada ne postoji državna organizacija kojoj je zadaća boriti se protiv INI-ja u kontekstu zaštite demokratskih vrijednosti i ugroze nacionalne sigurnosti. Sukladno dostupnim informacijama, za sada nije u planu osnivanje takve institucije, kao ni razvoj namjenske jedinice unutar postojećih državnih institucija koja bi imala zadaću razotkrivati dezinformacije i kreirati politike kojima bi se na državnoj razini suprotstavilo stvaranju i diseminaciji dezinformacija.

Problematika INI-ja u Hrvatskoj za sada je prepoznata u djelokrugu iz nadležnosti Ministarstva kulture i medija (MKM). MKM je u suradnji s Agencijom za elektroničke medije (AEM) poduzelo aktivnosti s ciljem povećanja otpornosti društva na



dezinformacije. Cilj se nastoji ostvariti smanjenjem količine INI-ja u javnom prostoru, jačanjem informacijske sigurnosti i pouzdanosti (pri konzumaciji medijskih sadržaja i prilikom korištenja internetskih društvenih mreža), porastom kvalitete novinarstva i vjerodostojnog izvještavanja te povećanjem medijske pismenosti građana Hrvatske. Tako je 2022. u okviru EU investicije „Uspostava provjere medijskih činjenica i sustava javne objave podataka” u sklopu Nacionalnog plana oporavka i otpornosti 2021. – 2026. (nositelji su MKM i AEM) izrađena u uvodu spomenuta studija *Jačanje otpornosti društva na dezinformacije: analiza stanja i smjernice za djelovanje*. Studija donosi pregled stanja i trendova u globalnom informacijskom kontekstu, obrađuje problematiku INI-ja na internetu, njegove karakteristike, smjer kretanja i dionike suvremenog informacijskog prostora te njihove međuodnose. U toj studiji sadržano je sedam preporuka za ključne aktivnosti u procesu jačanja otpornosti društva na INI: „(1) poticanje kvalitetnog i neovisnog novinarstva, (2) unaprjeđenje profesionalnih standarda u novinarstvu, (3) osnivanje neovisnih, specijaliziranih projekata provjere točnosti informacija, (4) jačanje povjerenja u provjeravatelje informacija (engl. *fact-checkers*), (5) sustavno osnaživanje građana vještinama medijske pismenosti, (6) razvoj računalno potpomognutih rješenja za borbu protiv dezinformacija, (7) jačanje suradnje ključnih dionika te sinergiju svih istraživačkih, razvojnih, edukativnih i *fact-checking* aktivnosti, za što je ključno osigurati potpore iz javnih sredstava, kroz sustav izravnih i neizravnih subvencija” (Grbeša Zenzerović i Nenadić, 2022: 77–78). Iz preporuka je jasno da se područjima ključnima za suzbijanje INI-ja smatraju novinarstvo, zatim organizacije za provjeru činjenica, operativne sustave za provjeru informacija i državne subvencije kojima bi se financirao njihov razvoj.

Međutim, razvoj operativnih sustava za provjeru informacija nije koncept koji na temelju zadanih parametara može jamčiti sigurno i učinkovito suzbijanje INI-ja. Također, organizacije za provjeru činjenica, ovisno o izvorima njihovog financiranja, kompetencijama za provjeru činjenicama te osobnim ideološkim, vjerskim i političkim uvjerenjima mogu biti slaba karika u aktivnostima jačanja otpornosti društva na INI. Preporuke također izostavljaju naglasiti potrebu suradnje s akademskom zajednicom koja je, kako se i u samoj studiji navodi, kod ključnih međunarodnih organizacija (Vijeće Europe, Europska komisija, UNESCO) prepoznata kao jedan od glavnih dionika u razvoju sustava utvrđivanja činjenica i provjere informacija. Osim razvoja sustava utvrđivanja činjenica i provjere informacija, akademska zajednica ključna je i u razvoju ostalih područja (ne)navedenih u preporukama kao što su novinarstvo, edukacija, znanstveno-istraživački rad, osnaživanje vještinama medijske pismenosti, razvoj računalno potpomognutih rješenja za borbu protiv dezinformacija i drugo. S obzirom na reference za izradu studije i metodološki pristup, razvidno je kako u izradi studije nisu konzultirani znanstvenici i stručnjaci iz područja informacijskih i komunikacijskih znanosti čiji je istraživački rad zasnovan na proučavanju informacija. S

druge strane, u studiji je u većoj mjeri naglasak stavljen na javne medije i novinarstvo. Promatrajući problematiku INI-ja iz tog rakursa propušta se uočiti šira slika negativnog utjecaja INI-ja na demokratska društva i nacionalnu sigurnost, a ne samo na novinarstvo i kvalitetu izvještaja. Kvalitetno, slobodno i neovisno novinarstvo bitno je za demokraciju, ali ako se INI promatra samo u kontekstu utjecaja na novinarstvo propustit će se šira slika, a to je da je INI ugroza za demokratsko društvo u cjelini.

Dezinformacije, pogrešne i zlonamjerne informacije u političkoj sferi imaju moć utjecaja na političke procese, nanose štetu demokracijama i građanima jer onemogućuju donošenje odluka zasnovanih na informacijama s integritetom. To je osobito slučaj u zemljama s niskom razinom medijske pismenosti te u manje demokratskim zemljama u kojima se dezinformacije često koriste kao oružje za diskreditaciju onih koji izražavaju stavove i poduzimaju aktivnosti koje su u suprotnosti s državnim vlastima i poslovnim interesima, otkrivaju korupciju i kršenja ljudskih prava te traže odgovornost političara (Turčilo i Obrenović, 2020). Uz navedeno, dezinformacijama se domaći i strani akteri služe da bi manipulirali procesima donošenja odluka u područjima od interesa, kao što su migracije, javna sigurnost, zdravstvo, financije, izborni procesi i drugo (Komunikacija Europske komisije, 2018).

Za učinkovito suzbijanje INI-ja u Hrvatskoj potrebno je javno identificirati ugrozu i izazove koje predstavljaju i prikazati ih kao politički problem. Time bi većina javnosti osvijestila da je posrijedi ugroza za demokraciju i nacionalnu sigurnost koja se može usporediti s oružanom agresijom. Poticanjem javne rasprave u koju bi bili uključeni dionici koji mogu pridonijeti svojim znanjem i iskustvom vrlo vjerojatno bi u javnosti podignula razinu svjesnosti o izazovima koje INI predstavlja. Kako bi ostvarila dublji uvid u stanje među građanima i donijela EU strategiju za suzbijanje širenja INI-ja na internetu, Europska komisija je 2018. provela ispitivanje javnog mnijenja koje je obuhvatilo 26 576 građana iz 28 država članica EU-a među kojima je i Hrvatska (Flash Eurobarometar 464, 2018). Rezultati ispitivanja javno su dostupni te u razvoju politika za suzbijanje širenja dezinformacija mogu biti od koristi donositeljima odluka i kreatorima politika u Hrvatskoj.

## Zaključak

Izazovi i ugroze proizašle iz INI-ja utječu na cjelokupno društvo te je u cilju jačanja otpornosti društva potreban sinergijski učinak različitih područja znanosti, državne uprave, javnih institucija, organizacija civilnog društva, medijskih organizacija i drugo. Slabljenje nacionalne sigurnosti, obrambenih sposobnosti i onemogućavanje procesa donošenja odluka u demokratskim društvima jedan je od ključnih razloga zbog kojih nastaju dezinformacije kao najopasnija vrsta INI-ja. Da je tomu tako dokazuje i pozornost koju su posljednjih godina dezinformacijama posvetili NATO i EU

prepoznajući ih kao problem sigurnosnog karaktera u okviru hibridnih prijetnji, informacijskih operacija ili zasebnih dezinformacijskih kampanja. Iako INI za sada u Hrvatskoj nije prepoznat kao sigurnosni izazov na razini državnih institucija, ostvareni su pomaci u pokretanju rasprava o njima i načinima njihovog suzbijanja u okviru MKM-a i AEM-a. S obzirom na to da je studija MKM-a i AEM-a izrađena u okviru djelokruga tih institucija, razumljivo je da u njoj nisu prepoznate i naglašene ugroze koje INI predstavlja za nacionalnu sigurnost demokracija. Potrebno je da se u raspravu o INI kao sigurnosnom problemu u Hrvatskoj uključe i akademska zajednica, državne institucije nadležne za pitanja sigurnosti i obrane kao i organizacije civilnog društva čiji rad je usmjeren prema područjima nacionalne sigurnosti i obrane.

Kada govorimo o vrstama, sa sigurnošću možemo reći da postoje dvije vrste INI-ja: dezinformacije i pogrešne informacije. U radu autori prikazuju tri vrste INI-ja od kojih su dezinformacije najopasnije za stabilnost demokracija i nacionalnu sigurnost demokratskih društava. Pogrešne informacije su određene terminološki i iznijeti su primjeri njihovog nastanka i pojave u hrvatskom medijskom prostoru. Također, analizirane su i zlonamjerne informacije za koje autori rada smatraju da je potrebna otvorena rasprava o tome mogu li se smatrati vrstom INI-ja ili su oblik u kojem se pojavljuju dezinformacije. Pojedini autori dezinformaciju određuju kao zlonamjernu informaciju te su stoga i zlonamjerne informacije dezinformacije. S druge strane, kako je prikazano u radu, neki autori smatraju da se dezinformacije i zlonamjerne informacije razlikuju jer su dezinformacije netočne i štetne informacije za razliku od zlonamjernih informacija koje su štetne, ali sadrže točne informacije. Zlonamjerne informacije (i lažne vijesti) termini su koji su se recentno pojavili u znanstvenoj literaturi i raspravama o INI-ju bez da su njihove osobine detaljnije analizirane, bez potvrde razlikovanja u odnosu na dezinformacije kao i bez znanstveno utemeljene potvrde njihovog mjesta među vrstama INI-ja. Nakon provedene analize i prikazane rasprave u članku, smatramo da postoje dvije vrste INI-ja koje su otprije prepoznate i obrađene u literaturi informacijskih i komunikacijskih znanosti. Zlonamjerne informacije zasad ne možemo sa sigurnošću odbaciti kao vrstu INI-ja, ali skloniji smo ih smatrati oblikom u kojem se pojavljuju dezinformacije, kao što su i lažne vijesti oblik dezinformacije.

Kako je prepoznato u EU-u i NATO-u, dezinformacijama je potrebno posvetiti najveću pozornost jer su najopasnija vrsta INI-ja kojima se može narušiti povjerenje u znanost i objektivne dokaze. Njihovo širenje i umnožavanje na internetu ugrožava demokratske procese i javna dobra kao što su sigurnost, zdravlje, gospodarstvo, pravosuđe, financije i okoliš. Ključ učinkovitog rješenja izazova koje predstavljaju dezinformacije u političkoj je volji i kontinuiranom provođenju politika koje će povećati medijsku pismenost i kolektivnu otpornost građana. Jedinstveno i jednostavno rješenje za suzbijanje dezinformacija ne postoji, ali to ne znači da se ne trebaju iznova pronalaziti nove politike koje bi sinergijskim djelovanjem postigle rezultate. Najveća

pogreška u suzbijanju dezinformacija bila bi odustajanje i nepoduzimanje mjera u cilju zaštite demokracije i njezinih vrijednosti. EU i NATO poduzeli su korake i državama članicama, među njima i Hrvatskoj, pokazale smjer u kojem je potrebno ići. Na Hrvatskoj je da kreira politike i poduzme mjere kako bi očuvala svoje nacionalne interese i demokratske vrijednosti.

## Literatura

- Akrap, G. 2009. Informacijske strategije i oblikovanje javnoga znanja. *National security and the future*, 10 (2): 77–151. <https://hrcak.srce.hr/80639>.
- Allcott, H. i Gentzkow, M. 2017. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, 31 (2): 211–236.
- Bennett, L. i Livingston, S. 2018. The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33: 122–139.
- Cordy Report 2017. *NATO Parliamentary Assembly – Committee on the Civil Dimension of Security. The Social Media Revolution: Political and Security Implications*. <https://www.nato-pa.int/document/2017-social-media-revolution-cordy-report-158-cdsdg-17-e-bis>. 10. rujna 2022.
- Domović, R. 2010. Inverzija istine – metoda ostvarivanja dominacije u javnom informacijskom prostoru. *National security and the future*, 11 (2–3): 61–108. <https://hrcak.srce.hr/80575>.
- Europska komisija. 2018. *A multi-dimensional approach to disinformation, Final report of the High Level Expert Group on Fake News and Online Disinformation (HLEG)*. <https://coinform.eu/wp-content/uploads/2019/02/EU-High-Level-Group-on-Disinformation-A-multi-dimensionalapproachtodisinformation.pdf>. 18. kolovoza 2022.
- Europska komisija. 2018. *Komunikacija Europske komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija – „Suzbijanje dezinformacija na internetu: europski pristup”*, COM (2018) 236 final, Bruxelles, 26. travnja 2018. [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=51804](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804). 9. rujna 2022.
- Europska komisija. 2018. *Flash Eurobarometer 464 (Fake News and Disinformation Online)*. GESIS Data Archive, Cologne. ZA6934 Data file Version 1.0.0, Bruxelles. <https://doi.org/10.4232/1.13019>. 27. siječnja 2023.
- Grbeša Zenzerović, M. i Nenadić, I. 2022. *Jačanje otpornosti društva na dezinformacije: analiza stanja i smjernice za djelovanje. Drugo, dopunjeno izdanje*. Zagreb: Agencija za elektroničke medije. [https://www.aem.hr/wp-content/uploads/2022/09/Studija\\_dezinformacije\\_2-izdanje.pdf](https://www.aem.hr/wp-content/uploads/2022/09/Studija_dezinformacije_2-izdanje.pdf).

- Gu, L., Kropotov, L., Yarochkin, F. 2017. *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public*. TrendLabs. [https://documents.trendmicro.com/assets/white\\_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf](https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf). 28. prosinca 2021.
- Hrvatska enciklopedija, mrežno izdanje. 2021. Leksikografski zavod Miroslav Krleža. *Dezinformacija*. <http://www.enciklopedija.hr/Natuknica.aspx?ID=14909>. 29. prosinca 2023.
- Jack, C. 2017. *Lexicon of Lies: Terms for Problematic Information*. *Data and Society*. Washington, DC.
- DORH 2020. *Javno priopćenje od 2. lipnja 2020*. <https://dorh.hr/hr/priopcenja/dorh-i-uskok-nisu-izvor-objavljenih-informacija-0>. 23. lipnja 2022.
- Jutarnji list*. 2020. <https://www.jutarnji.hr/vijesti/hrvatska/nisam-uhicen-nisam-optuzen-nisam-u-remetincu-slobodan-sam-hvala-hrt-u-15020234>. 5. rujna 2022.
- Klaić, B. 2012. *Novi rječnik stranih riječi*. Zagreb: Školska knjiga.
- Kovačić, S. 2021. *Online novinarstvo – Služenje javnosti ili podilaženje publici*. Zagreb: Hrvatska sveučilišna naklada – Sveučilište u Mostaru.
- Lippmann, W. 1922. *Public opinion*. New York: Harcourt, Brace and Company. <https://archive.org/details/publicopinion00lippgoog/page/n20/mode/2up?ref=ol&view=theater>. 18. siječnja 2022.
- Marević, J. 2000. *Latinsko-hrvatski enciklopedijski rječnik*. Zagreb: Matica Hrvatska.
- Merraim Webster Dictionary. *Disinformation*. <https://www.merriam-webster.com/dictionary/disinformation>. 5. rujna 2022.
- Moore, M. 2017. *Inquiry into Fake News. Culture, Media and Sport Select Committee*. London: Centre for the Study of Media, Communication and Power, King's College London.
- Nacional*. 2019. <https://www.nacional.hr/operacija-vukovar-vojni-obavjestajci-nezakonito-nadzirali-ekstremnu-desnicu/>. 10. siječnja 2022.
- Papa Franjo. 2018. *Poruka povodom 52. Svjetskog dana sredstava društvene komunikacije*. [https://www.vatican.va/content/francesco/hr/messages/communications/documents/papa-francesco\\_20180124\\_messaggio-comunicazioni-sociali.html](https://www.vatican.va/content/francesco/hr/messages/communications/documents/papa-francesco_20180124_messaggio-comunicazioni-sociali.html). 29. prosinca 2021)
- Sproule, M. J. 1997. *Propaganda and democracy: The American experience of media and mass persuasion*. Cambridge: University Press.
- Sapunar, M. 2004. *Osnove znanosti o novinarstvu*. Zagreb: vlastita naklada.
- Shmatenko, L. M. 2019. *Russian Disinformation Campaigns: What Risk for the European Union and the International Liberal Order?* Geneva: Global Studies Institute, University of Geneva.
- Tuđman, M. 2003. *Prikazalište znanja*. Zagreb: Hrvatska sveučilišna naklada.
- Tuđman, M. 2008. *Informacijsko ratište i informacijska znanost*. Zagreb: Hrvatska sveučilišna naklada.
- Tuđman, M. 2012. *Programiranje istine: Rasprava o preraspodjelama društvenih zaliha znanja*. Zagreb: Hrvatska sveučilišna naklada.

- Tuđman, M. 2014. *Teorija informacijske znanosti: treće dopunjeno izdanje*. Zagreb: Hrvatska sveučilišna naklada.
- Turčilo, L. i Obrenović, M. 2020. *Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy*. Heinrich Böll Foundation. [https://ps.boell.org/sites/default/files/importedFiles/2020/09/30/200825\\_E-Paper3\\_ENGL.pdf](https://ps.boell.org/sites/default/files/importedFiles/2020/09/30/200825_E-Paper3_ENGL.pdf). 10. siječnja 2022.
- The Aspen Institute 2021. *The Commission on Information Disorder Final Report*. [https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute\\_Commission-on-Information-Disorder\\_Final-Report.pdf](https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf). 11. siječnja 2022.
- Wardle, C. 2019b. *Understanding Information Disorder*. First Draft. <https://firstdraftnews.org/latest/information-disorder-the-techniques-we-saw-in-2016-have-evolved/>.
- Wardle, C. i Derakhshan, H. 2017. Information Disorder: Towards an Interdisciplinary Framework for Research and Policy-Making. *Council of Europe Report 27*. <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277>. 27. prosinca 2021.
- Weedon, J., Nuland, W. i Stamos, A. 2017. *Information operations and Facebook*. <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>. 5. rujna 2022.

## Integrity-breached information: Theoretical definition and threat to national security

### *Abstract*

We consume much information in the current information realm, including integrity-breached information. Although information manipulation in the public sphere is not new, the volume and speed at which it spreads through online social networks and communication platforms pose a fresh challenge and threat to the security of democratic countries. To communicate that the integrity of published information is severely compromised, various terms are employed in the public, leading to terminological and cognitive misunderstanding. The integrity-breached information types, such as misinformation, malinformation, and disinformation, are examined and theoretically determined in this paper. The paper then provides examples of institutional challenges to tackling the dissemination of integrity-breached information on the internet and illustrates the threat they represent to the national security of democratic societies.

**Key words:** integrity-breached information, disinformation, misinformation, malinformation, national security, information and communication science.