SKUP ALATA ZA PROVJERU ČINJENICA

Vilnius, studeni 2025.

Konsolidirani vodič za metodologije, alate i resurse za učinkovitu provjeru činjenica

ATEITININKŲ FEDERACIJA, LITVA
PROJEKT DECIDE

Co-funded by the European Union

Tablica sadržaja

Uvod 2
Temeljni i ključni pojmovi 5
Početak provjere činjenica 9
Radni procesi 14
Alati i tehnike 18
Europske studije slučaja 22
Priručnik za zemlju 25
Zaključak 27
Prilozi 28

u ime obitelji
World Youth Alliance Southeast Europe
PLATTFORM CHRISTDEMOKRATIE
ATEITININKAI

Co-funded by the European Union

Uvod

O programu ambasadora za provjeru činjenica

Provjera činjenica je proces provjere jesu li tvrdnja, slika, statistika ili priča točne. To znači praćenje informacija do vjerodostojnih primarnih izvora, provjeru konteksta i jasno označavanje onoga što je istinito, lažno, obmanjujuće ili nedokazano – transparentnim dokazima.

Zašto je to danas toliko važno?

Preopterećenost informacijama: Svakodnevno smo izloženi tisućama postova; laži se šire brže od ispravaka.

Sadržaj generiran umjetnom inteligencijom: Deepfakeovi i sintetički tekst čine da lažnjaci izgledaju uvjerljivo.

Odluke s visokim ulozima: Loše informacije mogu utjecati na izbore, zdravstvene izbore i javnu sigurnost.

Povjerenje i odgovornost: Rigorozna provjera obnavlja povjerenje u institucije i medije.

Građanska otpornost: Javnošću koja je pismena o činjenicama teže je manipulirati.

Program ambasadora provjere činjenica stvoren je kako bi se ojačala medijska pismenost, kritičko razmišljanje i građanska otpornost diljem Europe. Nudi strukturiran, ali prilagodljiv okvir koji pomaže sudionicima da prepoznaju, provjere i odgovorno prenesu točne informacije. Metodologija identificira devet smjernica i ostvaruje ih kroz četiri integrirana provedbena dijela.

Ovaj je materijal sastavljen na temelju materijala predstavljenog tijekom događaja uživo – Radionica medijske pismenosti: Kako prepoznati i boriti se protiv dezinformacija – održanog u Vilniusu, Litva, od 10. do 12. listopada 2025. i dopunjen javnim izvorima informacija na temelju preporuka predavača. Za obradu informacija korišteni su alati umjetne inteligencije.

Zahvaljujemo prof. dr. Dariusu Pilkynasu i izv. prof. Liutaurasu Ulevičiusu s Fakulteta za komunikacije Sveučilišta u Vilniusu, Joviti Tautkevičiūtė-Kalinauskienė iz projekta Debunk.org na dostavljenom teorijskom materijalu i Arnasu Jasinskasu iz Federacije budućnosti na održavanju živahnog seminara o dezinformacijama, čiji su uvidi također bili korisni u pripremi ovog skupa alata.

Vizija

Glavna vizija programa ambasadora provjere činjenica je opremiti pouzdane članove zajednice za otkrivanje, provjeru i odgovorno komuniciranje činjenica – kako bi zajednice postale otpornije na mis/dezinformacije i mogle donositi bolje odluke.

Ciljevi programa

Znanje: Sudionici mogu definirati misinformacije/dezinformacije/propagandu; opisati uobičajene taktike; objasniti osnove ABCDE-a i OSINT-a.

Vještine: Sudionici mogu pokrenuti trijažu od 5 do 10 minuta, provjeriti slike/videozapise/tekst i dokumentirati transparentan lanac zaključivanja.

Stavovi: Sudionici postupaju s poštovanjem, izbjegavaju sukobe i daju prednost jasnoći, empatiji i točnosti.

Praksa: Svaki sudionik izrađuje jednu kratku provjeru činjenica i jedan akcijski plan informiranja prilagođen njihovoj zajednici.

Porast: Najmanje jedna lokalna mikro-obuka (60-90 min) održana u roku od 60 dana nakon certifikacije.

Čemu služi ovaj skup alata

Ovaj skup alata pomaže ambasadorima da kritičko razmišljanje pretvore u dosljednu svakodnevnu praksu: kako uočiti upitne tvrdnje, učinkovito ih provjeriti i odgovorno komunicirati nalaze unutar svoje nevladine organizacije i širih zajednica. Prvi je zadatak: kratka objašnjenja, zatim konkretne radnje koje možete poduzeti u 5/10/30 minuta, plus primjeri i radni listovi. Pročitajte ga jednom kako biste naučili kartu, a zatim se vratite kada planirate treninge, reagirate na incidente ili mentorirate nove ambasadore. Tretirajte ga kao praktični terenski priručnik, a ne kao čitač teorije i oslonite se na brze kartice i poveznice. Rezultat je zajednički jezik, jasni radni procesi i osnova za kvalitetu.

Koristit ćete ga za:

Brzu procjenu tvrdnji i izvora, čak i pod vremenskim pritiskom.

Odabir pravih alata za provjeru i radne procese.

Jasno i s poštovanjem ojašnjavanje svog razmišljanja osobama koje nisu stručnjaci.

Podršku komunikaciji vaše nevladine organizacije pouzdanim, dokumentiranim provjerama.

Što se nalazi unutar ovog skupa alata

Skup alata je usirden u jasnim konceptima – misinformacijama, dezinformacijama i malinformacijama – i navikama kao što su lateralno čitanje i provjere podrijetla, inokulacija/prethodno otkrivanje dezinformacija (prebunking) i rigorozna trijaža izvora, a sve s ciljem da se svaka provjera učini ponovljivom. Predstavlja moderne dezinformacije kao brz, skalabilan sustav u kojem su privlačenje pažnje i znakovi identiteta važniji od medija te naglašava da transparentna provjera, arhiviranje i standardi podrijetla ostaju najbolja snaga.

Praktična ABCDE leća prebacuje rad s post-by-post reakcija na svijest o sustavu: Akter, Ponašanje, Sadržaj, Stupanj, Učinak – koristi se za odabir hoće li/gdje intervenirati i koliko snažno. Sekcija također pokriva zašto ljudi vjeruju u neistine (pristranost potvrde/dostupnosti, motivirano rasuđivanje, klasična propagandna sredstva) i poziva na istinu na prvom mjestu i poruke pune poštovanja kako bi se izbjegao povratni učinak. Objašnjava ulogu umjetne inteligencije u generiranju i širenju (sadržaja) te propisuje protupoteze: provjera podrijetla, korištenje vizualne/audio forenzike (ključni kadrovi, obrnuta pretraživanja), arhiviranje svakog koraka i komuniciranje neizvjesnosti.

Vremenski ograničeni radni procesi 5/10/30 pretvaraju teoriju u ponovljivu akciju. 5-minutna SIFT trijaža sprječava slučajnu manipulaciju; 10-minutni tijek daje kratku presudu s oznakom pouzdanosti; 30-minutna provjera dokumentira ABCDE, kontekst, etiku i proporcionalni odgovor, s predloškom za objašnjenje spremnim za javnost.

„Alati i tehnike“ detaljno opisuju praktične upute: trijaža podrijetla i izvora, pretraživanje obrnutih slika i ključnih kadrova, provjera citata/brojeva, forenzika domene/web stranice za klonove/tipfelere, trijaža društvenih mreža, OSINT geo/krono provjere, otkrivanje uzoraka kampanje vezano za ABCDE, leća ranjivosti za prilagođavanje odgovora i strogo arhiviranje/sljedivost. Također uključuje podsjetnik „što koristiti kada“ i matricu odgovora za usklađivanje stupanj × učinak s radnjama koje najmanje pojačavaju (situaciju). Etičke i obvezne mjere zaštite – minimiziranje štete, zaštita privatnosti, prikazivanje nesigurnosti i poštivanje pravila o podacima – plus kontrolna lista kvalitete čine rezultate sigurnijima i ponovljivijima.

Konačno, europski snimci slučajeva (npr. Operacija Doppelgänger, MH17, Slovačka 2023 deepfake audio, Zelensky deepfake, LT hibridni pushovi) pretvaraju metode u mišićnu memoriju kroz 30-minutne radionice (laboratorijske vježbe) koji kombiniraju provjeru, ABCDE mapiranje i proporcionalni odgovor.

Temeljni i ključni pojmovi

Prije nego što bilo što provjerite, važno je razumjeti s kojom vrstom informacija imate posla. Jasne definicije sprječavaju zabunu i održavaju rasprave produktivnima. Koristite ih tijekom planiranja i izvještavanja te unakrsno povežite pojmove u svojim internim dokumentima. Pazite na uobičajene zabune poput namjere (mis vs. dezinformacije) i zanemarivanja malinformacija. Svaki unos treba sadržavati primjer u dva retka i poveznicu na „vidi također" metode.

Vrste lažnih ili obmanjujućih informacija:

Misinformacije – lažne, ali podijeljene bez namjere nanošenja štete.

Dezinformacije – lažni sadržaj koji se dijeli s namjerom obmane.

Malinformacije – prave informacije koje se koriste izvan konteksta kako bi se nanijela šteta (npr. doxing).

Ostali važni pojmovi:

Verifikacija nasuprot validaciji: Verifikacija provjerava činjenice (što se dogodilo?). Validacija provjerava zaključak i metodu (podupiru li dokazi tvrdnju?).

Lateralno čitanje i podrijetlo: Umjesto da ostanete na jednoj stranici, otvorite nove kartice kako biste provjerili tko je izvor. Prije nego što se uključite u sadržaj, utvrdite tko/što/gdje/kada/zašto.

Inokulacija/prethodno otkrivanje dezinformacija(prebunking): Upozoravanje ljudi *prije nego* što naiđu na manipulaciju. Kratko, proaktivno upozorenje + primjer tehnike manipulacije za izgradnju otpora prije izlaganja.

Trijaža izvora: tko je objavio, dosadašnji rad, kvalifikacije/stručnost, financiranje, tko je podijelio.

Društvene ranjivosti: polarizacija, niska medijska pismenost, nejednakost, slaba kibernetička sigurnost, nisko institucionalno povjerenje, slaba regulacija platforme → veći FIMI rizik.

Sljedivost: Svaku tvrdnju koju objavite mora moći reproducirati kolega koristeći vaše bilješke, veze i arhivirane snimke.

Pogledajte Rječnik za sažete definicije i primjere.

Kratka povijest modernih dezinformacija

Preddigitalni korijeni (kraj 19. – sredina 20. st.). Mnogo prije interneta, države i politički pokreti naučili su naoružati glasine, krivotvorene dokumente i masovne medije. Ranih 1900-ih vidjela se propaganda industrijskih razmjera u novinama i plakatima; Prvi i Drugi svjetski rat profesionalizirali su tehnike poput emocionalnog uokvirivanja, selektivne statistike i demonizacije vanjskih skupina. Radio i filmski žurnali smanjili su troškove distribucije i povećali uloge: ako biste mogli zauzeti toranj za emitiranje, mogli biste preko noći oblikovati stvarnost za naciju. Ova razdoblja uče dvije trajne lekcije: mediji se mijenjaju, ali psihološke poluge – strah, identitet, pritužba – nevjerojatno su stabilne; a kontrola distribucije je moć.

"Aktivne mjere" Hladnog rata (1945.–1991.). Službe Sovjetskog saveza i Varšavskog pakta vodile su višegodišnje kampanje utjecaja kombinirajući krivotvorine, naslovnice i podmetnute priče. Najpoznatija je bila operacija KGB-a/Stasija protiv AIDS-a: počevši od sredine 1980-ih, operativci su širili članke koji su tvrdili da je HIV američko biološko oružje, perući tu tvrdnju putem stranih novina i pseudo-stručnjaka sve dok nije odjeknula globalno. Nakon Hladnog rata, dužnosnici su potvrdili autorstvo operacije; povjesničari su kasnije pojasnili njezin kodni naziv kao Operacija Denver (popularno poznata kao Operacija INFEKCIJA). Šteta kampanje za javno zdravstvo – poticanje nepovjerenja i rizičnog ponašanja – ostaje upozoravajuća priča o stvarnim svjetskim troškovima dezinformacija.

Komercijalni internet i era pretraživanja (1990-te – 2008.). Mreža(Web) je preuredila kontrolu informacija (gatekeeping). Tražilice i rani forumi stvorili su nove poticaje: privlačenje pozornosti, visoki rang, monetizacija putem oglasa. "Farme sadržaja" i blogovi niskog trenja zamaglili su granice između mišljenja, glasina i izvještavanja. Forumi i lančani e-mailovi socijalizirali su "vjerodostojnost među ravnopravnima" (peer-to-peer credibility), gdje familijarnost često zamjenjuje provjeru. Obrazac koji se ovdje pojavljuje – optimizirati za klikove, a zatim popuniti narativ – samo će se pojačati na društvenim platformama.

Uspon platforme i algoritamski feedovi (2008. – 2013.). Facebookov News Feed, preporuke na YouTubeu i popisi trendova na Twitteru učinili su distribuciju personaliziranom i neprozirnom. Mikrociljani oglasi omogućuju akterima testiranje i ponavljanje poruka po niskoj cijeni. Model upravljanja platformom – reaktivan, u masovnim razmjerima – borio se da održi korak s koordiniranim mrežama, lažnim mrežnim identitetom (sockpuppets) i „hakiranjem angažmana“ koje iskorištava novost, skandal i identitet.

Umrežene operacije postaju mainstream (2014. – 2018.). Ruske informacijske operacije oko Ukrajine i zapadnih izbora pokazale su koordinaciju na više platformi. Agencija za istraživanje interneta (IRA) pokrenula je tisuće osoba, stranica i grupa kako bi iskoristila društvene podjele; američke istrage i Obavještajni odbor Senata dokumentirali su doseg i taktike, dok su platforme započele velika rušenja imovine IRA-e. Paralelno s tim, obaranje MH17 iznad Ukrajine 2014. pokrenulo je brzi ciklus konkurentskih narativa, lažnih slika i službenog

zamagljivanja; istražitelji otvorenog koda (posebno Bellingcat) suprotstavili su se geolokacijom, praćenjem oružanih sustava i rekonstrukcijom slijeda događaja, što je ključni trenutak za ulogu OSINT-a u razotkrivanju državnih dezinformacija.

Šifrirani razgovori, rubne platforme i "infodemija" (2019. – 2021.). Aplikacije za razmjenu poruka i alternativne platforme smanjile su vidljivost moderiranja i povećale viralnost u zatvorenim mrežama. Tijekom COVID-a 19, WHO je krizu označila kao infodemiju – preobilje informacija (istinitih, lažnih i svega između) koje su stvorile zbunjenost i opasno ponašanje. Doba pandemije normaliziralo je „dokaze oblikovane kako bi odgovarale identitetu“, gdje su zajednice sastavljale prilagođene stvarnosti iz memeova, videozapisa i lažiranih snimaka zaslona brže nego što su institucije mogle odgovoriti.

Rat i platforme susreću OSINT u velikim razmjerima (2022.–2023.). Potpuna invazija Rusije na Ukrajinu ubrzala je i manipulaciju i protumanipulaciju. Mreže utjecaja vodile su klonirane portale i stranice za lažno predstavljanje – najvidljivija je bila operacija Doppelgänger, koja je lažirala europske medije i ministarstva kako bi podmetnula antiukrajinske narative i narušila podršku. Istražitelji i vlade razotkrili su kombinaciju tehnika: slične domene, kopirani predlošci stranica, posijane priče i kupnje oglasa kako bi se povećao doseg. U međuvremenu, zajednice otvorenog koda i profesionalne redakcije spojile su metode – satelitske snimke, podatke senzora, video s terena – kako bi opovrgnule tvrdnje u približno stvarnom vremenu, pomičući ravnotežu informacija prema transparentnoj provjeri.

Era generativne umjetne inteligencije (2023.–2025.). Jeftina sinteza promijenila je krivulju troškova. Tekst, slike, glasovi i videozapisi sada se mogu izmišljati ili suptilno mijenjati u velikim razmjerima; akteri s malo truda mogu voditi kampanje „kvantiteta nad kvalitetom“ koje se čine dovoljno autentičnima da prođu ležerno listanje (skrolanje). Izbori u stvarnom svijetu počeli su bilježiti konkretne štete: u siječnju 2024. robotski pozivi generirani umjetnom inteligencijom koji oponašaju predsjednika Bidena pokušali su obashrabriti izlaznost u New Hampshireu; američki regulatori odgovorili su zabranom glasova umjetne inteligencije u robotskim pozivima i provođenjem novčanih kazni i podizanjem optužnica protiv uključenih organizatora i operatera. U isto vrijeme, platforme i izdavači počeli su pilotirati alate za podrijetlo kao što su C2PA/Content Credentials, koji ugrađuju provjerljive povijesti uređivanja u medijske datoteke; pristup je obećavajući, ali ovisi o usvajanju ekosustava i jasnoći korisničkog sučelja.

Europski regulatorni zaokret (2022. – 2025.). EU je dobrovoljne mjere nadopunila obvezujućim pravilima. Ojačani kodeks dobre prakse protiv dezinformacija (2022.) potaknuo je obveze demonetizacije i transparentnosti među platformama, oglašivačkim mrežama i provjeravateljima činjenica, dok evaluacije ističu neujednačenu usklađenost. Aktom o digitalnim uslugama (DSA) utvrđene su pravne obveze i provedbene ovlasti – koje se u potpunosti primjenjuju na platforme od 17. veljače 2024. – uključujući procjene sistemskog rizika (npr. dezinformacije), pristup podacima za provjerene istraživače i znatne novčane kazne

za prekršaje. Istraživači i civilno društvo sada istražuju koliko ove mjere smanjuju monetizaciju i posežu za dezinformacijama u praksi, dok regulatori testiraju DSA u odnosu na stvarne slučajeve (uključujući operacije u stilu "Doppelgänger").

Što se zapravo promijenilo – a što nije. Medij je evoluirao od tiska, preko emitiranja, do feedova i temeljnih modela (umjetne inteligencije), ali se „knjiga pravila“ i dalje vrti oko privlačenja pažnje, signala identiteta i ponavljanja narativa. Jeftinost stvaranja sadržaja i netransparentnost kuriranja (sustavi preporuka, privatne grupe, šifrirani kanali) pomaknuli su teren prema opsegu i brzini. Ipak, transparentna verifikacija, otvoreni arhivi i standardi podrijetla daju braniteljima prednost – posebno kada su upareni s „prebunkingom“ i glasnicima ukorijenjenim u zajednici. Ono što je značajno, mjerljivi učinci izloženosti sadržaju stranog utjecaja mogu biti manji nego što se strahuje na individualnoj razini; društvena opasnost je agregat: narativna zasićenost koja nagriza zajedničke činjenice i oduzima institucionalno vrijeme.

Početak provjere činjenica

Prije nego što započnemo s procesom provjere činjenica, shvatimo kako dezinformacije funkcioniraju i zašto čak i inteligentni ljudi vjeruju u laži. Ukratko ćemo razgovarati o tome kada i kako reagirati te o etici provjere činjenica.

Nakon usklađivanja koncepata, prijeći ćemo na radne procese 5/10/30 tijekom rada uživo. Posavjetujte se s alatima i tehnikama za specifične metode i proučite europske studije slučaja za end-to-end (cjelovite) primjere. Održavajte ciklus živim ugradnjom nalaza u buduća poboljšanja. Na kraju, predstavljamo priručnike za zemlje koje sudjeluju u našem projektu, koji pokazuju kako lokalizirati ranije spomenute godine i koje pouzdane izvore koristiti. Na temelju primjera možete izraditi priručnik za bilo koju zemlju. Ukratko:

1. Počnite ovdje kako biste se uskladili s konceptima i etikom.
2. Prijeđite na radne procese (10/5/30) za postupke korak po korak.
3. Posavjetujte se s alatima i tehnikama za specifične verifikacije (slike, brojevi, citati, mreže).
4. Proučite europske studije slučaja kako biste vidjeli end-to-end (cjelovite) radne procese.
5. Pogledajte priručnik za rad u zemlji na vašoj određenoj lokaciji

Kako funkcionira dezinformacija

Dezinformacija nije samo lažna objava ili lažna slika – to je **sustav**. Širi se zbog načina na koji je informacija stvarana, dijeljena i reagirana na mreži. Razumijevanje načina na koji ovaj sustav funkcionira pomaže ambasadorima da brzo prepoznaju obrasce i odaberu pravi odgovor.

1. Počinje s akterom

Netko stvara ili širi obmanjujući sadržaj. To može biti:

- Pojedinac sa snažnim mišljenjima
- Koordinirana skupina ili mreža
- Bot ili automatizirani račun
- Medijska kuća s vlastitim ciljevima
- Državni akter koji pokušava utjecati na mišljenje

Ključno pitanje: *Tko ima koristi ako ljudi vjeruju u to?*

2. Koristi strateško ponašanje

Dezinformacije se rijetko šire slučajno. Uobičajena ponašanja uključuju:

- Objavljivanje iste poruke na mnogim računima

- Korištenje emocionalnog jezika za izazivanje reakcija
- Automatizacija postova za povećanje opsega
- Plaćanje oglasa ili promoviranje sadržaja
- Preusmjeravanje korisnika putem sumnjivih poveznica

Ova ponašanja pomažu lažnim tvrdnjama da brže dopru do većeg broja ljudi.

3. Sadržaj je oblikovan tako da izaziva emocije

Dezinformacija najbolje djeluje kada ljudi osjećaju:

- Uvredu
- Strah
- Ponos
- Ugroženost ili nesigurnost

Snažne emocije uzrokuju da ljudi dijele prije razmišljanja. Često se koriste slike, kratki videozapisi i jednostavni slogani jer zaobilaze kritičko razmišljanje.

4. Cilj je pažnja, a ne točnost

Dezinformacija se širi jer platforme nagrađuju:

- Angažman
- Klikove
- Dijeljenja
- Komentare

Što je sadržaj emotivniji ili senzacionalniji, algoritam ga više gura. Lažni sadržaj ne mora biti uvjerljiv – samo treba privlačiti pažnju.

5. Stupanj: Širi se mrežama

Jedna objava možda neće nanijeti štetu, ali mreže mogu:

- Ponoviti istu poruku s različitih računa
- Koordinirati objavljivanje u određeno vrijeme
- Koristiti influencere kako bi joj dali kredibilitet
- Premjestiti isti narativ na različite platforme (FB → TikTok → Telegram)

Ovo ponavljanje čini poruku poznatom i stoga „istinitom".

6. Učinak: Cilj je utjecati na uvjerenja ili ponašanje

Dezinformacijom se nastoji:

- Narušiti povjerenje u institucije
- Povećati polarizaciju
- Obeshrabriti glasovanje ili sudjelovanje
- Širiti strah ili neizvjesnost
- Manipulirati javnim mnijenjem ili ponašanjem

Utjecaj može biti mali za pojedinačnu osobu, ali velik na razini zajednice.

7. Zašto ljudi vjeruju u to

Korisnici su ranjivi kada sadržaj:

- Potvrđuje njihova postojeća uvjerenja
- Odgovara njihovom svjetonazoru
- Čini se da dolazi od nekoga "poput njih"
- Prikazuje dramatičnu priču ili šokantnu sliku

To je normalna ljudska psihologija – nije mana.

8. Dobra vijest: jednostavne provjere djeluju

Većina dezinformacija može se rano zaustaviti:

- Provjerom izvora
- Traženjem izvorne slike ili videozapisa
- Traženjem ranijih verzija zahtjeva
- Pauziranjem prije dijeljenja
- Pitanjem: *Koja je namjera iza ovog posta?*

Dezinformacija se oslanja na brzinu. Provjeravatelji činjenica oslanjaju se na jasnoću. Usporavanje čak i na 10 sekundi prekida ciklus.

ABCDE leća je praktičan *način da „vidite sustav" iza jedne tvrdnje, ABCDE vas prebacuje s post-by-post reakcija na svijest o sustavu: akter, ponašanje, sadržaj, stupanj i učinak. Pokrenite ga prije nego što uložite resurse kako bi se trijaža i strategija uskladili. Nemojte se fiksirati samo na sadržaj – signali o akterima i potencijalnim učincima često određuju proporcionalne odgovore. Svaka upotreba trebala bi završiti kratkom preporukom što dalje.*

A – Akter (Actor): Tko stvara/širi sadržaj? Pojedinac, koordinirana mreža, bot, medijska kuća, nevladina organizacija, državni akter? Kakvi su njihovi rezultati i objavljeni interesi?

B – Ponašanje (behaviour): Učestalost objavljivanja, koordinacija na više platformi, lažna podrška, organizirano napadanje, signali slični botovima, obrasci monetizacije.

C – Sadržaj (content): Što se tvrdi? Točne formulacije, korišteni podaci, uređivanja, vizualni elementi, emocionalni okidači, nedostajući kontekst.

D – Stupanj (degree): Koliko je raširen i utjecajan? Je li to niša, u trendu ili mainstream? Koja je ciljana publika?

E – Učinak (effect): Kakva bi šteta mogla nastati (sigurnost, javno zdravlje, građansko povjerenje)? Koje su protumjere proporcionalne?

Koristite ABCDE da odlučite hoćete li intervenirati, koliko snažno i gdje (javna objava, privatna poruka, organizacijska izjava, zahtjev medija).

Ljudska psihologija: zašto pametni ljudi vjeruju lažnim stvarima

Vjerovati lažnim informacijama ne znači da je netko neobrazovan ili neinteligentan. Zapravo, pametni ljudi mogu biti jednako ranjivi - ponekad čak i više. To se događa jer dezinformacija djeluje u skladu s ljudskom psihologijom, a ne protiv nje. Pristranosti, identitet i emocije oblikuju način na koji ljudi primaju ispravke. Provjerite svoje poruke u odnosu na uobičajene zamke i klasične propagandne taktike kako bi bile učinkovite i ne bi imale suprotan učinak. Izbjegavajte posramljivanje i ponavljanje lažne tvrdnje u naslovima. Težite objašnjenjima koja su na provm mjestu istinita, uvažavajuća i pozivaju na dijalog.

- Kognitivne pristranosti:
    - Pristranost potvrde (tražimo dokaze s kojima se već slažemo)
    - Pristranost dostupnosti (nedavne ili živopisne priče čine se vjerojatnijima)
    - Pristrano razmišljanje (branimo svoj identitet, a ne činjenice)
- Propagandna sredstva (klasična taktika): etiketiranje, svjetlucave općenitosti, prijenos (asocijacija), svjedočanstvo (preporuka), obični ljudi, slaganje karata (selektivno iznošenje činjenica), efekt krda (svi to rade).
- Emocionalna dinamika: strah, bijes i ponos identitetom povećavaju mogućnost dijeljenja (sadržaja) i smanjuju kritičko preispitivanje.

Praktična implikacija: Ambasadori bi trebali upariti verifikaciju s empatičnom komunikacijom – predvodeći jasnoćom, a ne prezirom. Usredotočite se na dijeljenje provjerene istine, a ne na dokazivanje drugima da su u krivu. Izbjegavajte sramoćenje - to zatvara razgovor. Koristite jasna, jednostavna objašnjenja. Bavite se emocijama, a ne samo činjenicama.

Razumijevanje ovih psiholoških točaka pomaže vam da komunicirate na način na koji ljudi zapravo mogu čuti. Istina se najbolje širi kada se doživljava kao puna poštovanja, ljudska i bliska.

Odlučivanje kada i kako odgovoriti

Uskladite intenzitet odgovora stvarnom riziku i dosegu (sadržaja) kako biste izbjegli pojačavanje minornog sadržaja. Kombinirajte „stupanj“ i „učinak“ kako biste odabrali između privatnog pojašnjenja, kratkog javnog posta, cjelovitog objašnjenja ili koalicijske poruke. Budite oprezni s citiranjem na Twitteru ili ponavljanjem laži. Postavite plan nadzora koji precizira tko provjerava što, gdje i koliko često.

- Intervenirajte kada: narativ dobiva na snazi, šteta je vjerojatna, vaša nevladina organizacija je imenovana ili je vaša zajednica na meti.
- Uskladite odgovor na rizik:
    - Nizak rizik, nizak doseg: tiho pojašnjenje pojedincu.
    - Srednji rizik: kratka javna objava s jasnim ispravkom i jednom mjerodavnom poveznicom.
    - Visoki rizik / koordinirano: cjelovito objašnjenje, koalicijske poruke, angažman medija i proaktivno razotkrivanje.
- Izbjegavajte zamke: nemojte ponavljati lažnu tvrdnju u naslovima; predvodite istinom, a zatim se osvrnite na laži.

Etika i obveza zaštite

Pravila štite dostojanstvo, sigurnost i povjerenje dok provjeravate (činjenice) i komunicirate. Prije objavljivanja pitajte smanjujete li štetu, jeste li transparentni u pogledu neizvjesnosti, štitite li volontere i pridržavate li se zakonskih pravila i pravila brenda. Izbjegavajte „doxing“, nepotrebne osobne podatke i probleme s GDPR-om; dokumentirajte uznemiravanje i prijavite prijetnje. Koristite etički kontrolni popis, sigurnosni protokol i kratku bilješku o usklađenosti.

- Poštovanje i dostojanstvo: Kritika tvrdi, a ne ljudi.
- Proporcionalnost: Razmotrite nenamjernu manipulaciju; odaberite kanale u skladu s tim.
- Transparentnost: Podijelite metode, izvore i nesigurnost.
- Sigurnost: Zaštitite identitet volontera gdje je to potrebno; dokumnetirajte uznemiravanje; prijavite prijetnje.
- Usklađenost: Slijedite pravila brenda, pravnim propisima i pravilima o zaštiti podataka svoje organizacije.

Radni procesi

Radni procesi od 5/10/30 minuta naši su vremenski ograničeni priručnici za provjeru činjenica pod pritiskom stvarnog svijeta: 5-minutna SIFT trijaža kako bi se izbjegla slučajna manipulacija, 10-minutna koncizna provjera koja daje kratki zaključak koji se može povezati s oznakom pouzdanosti i 30-minutna potpuna provjera koja dokumentira dokaze, kontekst (ABCDE), etiku i proporcionalni odgovor. Uključujemo ih kako bismo dobre namjere pretvorili u ponovljivu akciju – tako da svaki ambasador, bez obzira na iskustvo, može slijediti iste korake, postići dosljednu kvalitetu, ostaviti transparentan revizijski trag i odabrati najmanje manipulacijski odgovor koji još uvijek štiti povjerenje naše zajednice.

Na kraju ovog odjeljka pružamo i kratke vodiče (tutoriale) koji se mogu učinkovito koristiti u stvarnom vremenu za odgovor na dezinformacije i koji mogu biti korisni u procesu učenja.

Evo osnovnih 5/10/30-minutnih tijekova rada za vaš skup alata.

5 minuta — SIFT brza trijaža (prije dijeljenja/prosljeđivanja)

Cilj: Odlučiti „ignoriraj / spremi za kasnije / brzo razjasni“ bez upadanja u zamke.

1) Stanite. Dišite. Ne širite dalje. Snimite post/vezu/snimku zaslona (URL + vremenska oznaka). Ako se radi o storiju/reelu, snimite zaslon i zabilježite vrijeme.

2) Istražite izvor. Tko ga je objavio? Kakvi su njihovi dosadašnji rezultati/stručnost? Kako se financiraju? Tko ga je dalje dijelio i zašto? Ako tvrdi da je poznati medij ili novinar, provjerite službenu stranicu za kontakt i usporedite domene (uočite tipfelere/klonove/lažno predstavljanje).

3) Pronađite bolje izvještavanje. Otvorite dvije neovisne kartice (lateralno čitanje). Pretražite osnovnu formulaciju tvrdnje + operatori web-lokacije. Potražite primarne ili mjerodavne izvore (službene statistike, izjave sudova/vlasti, renomirane medije).

4) Pratite do izvora. Pomaknite se do najranije verzije koju možete pronaći. Ako vizualno: brzo pokrenite Google Lens/TinEye - vidite li ranije datume ili različite kontekste?

5) Odlučite + zabilježite rizik. Ako miriše na element kampanje (botovi, navala identičnih kopija, influencerski vrući pokušaji, „previše uglađena“ stranica za kloniranje), nemojte se još javno angažirati. Zapišite: vrsta zahtjeva (događaj/broj/citat/slika/video), povjerenje (nisko/nepoznato) i može li to utjecati na poznate društvene ranjivosti (polarizacija, niska medijska pismenost, nisko povjerenje itd.).

Rezultati (≤60 riječi): trijažna bilješka u jednom odlomku s poveznicom/ama, najranija pojava, brzi zaključak o izvoru i sljedeća radnja (zanemari / pitaj privatno / 10-minutna provjera).

10 minuta — Koncizna verifikacija (mikronalaz koji se može objaviti)

Cilj: Proizvesti kratak rezultat koji se može povezati s oznakom pouzdanosti.

0) Postavljanje. Napravite mini dnevnik: zahtjev, URL-ovi, snimak/ke zaslona, vremenska/e oznaka/e. Arhivirajte ključne veze (Wayback ili Perma.cc). Klasificirajte: mis / dis / mal / neprovjereno.

1) Klasificirajte vrstu zahtjeva i odaberite pravi mikroalat. Slika: Spremite datoteku → Google Lens/TinEye → usporedite najraniju upotrebu i podudaranja više rezolucije → provjerite ima li izrezivanja/uređivanja.

- Videozapis: izdvojite 3 – 5 ključnih kadrova (desni klik na kadar ili alat za ključne kadrove) → obrnuto pretraži kadrove. Skeniranje tragova umjetne inteligencije pokazuje: nepodudarnost sinkronizacije usana/audio-video, stakleni pogled, preglatka koža, deformirane ruke, pretjerano čist/monoton glas.
- Citat/"X je rekao Y": Pretražujte točnu frazu u navodnicima + stranica: službenih stranica ili renomiranih medija.
- Broj/statistika: Identificirajte primarni skup podataka; provjerite najnoviju službenu publikaciju (metoda, vremenski raspon, upozorenja).
- Račun/izvor: Provjerite starost domene/registratora, TLS certifikat, stranicu za opis/kontakt, potpise autora. Usporedite s web mjestom legitimnog medija (otkrijte klonirane izglede/tipfelere). Bacite pogled na povijest objava radi navala copy-paste-a te koordiniranih hashtagova (pokazatelj ponašanja).

2) Unakrsna provjera. Otvorite najmanje dvije neovisne potvrde (autoritet + ugledno izvještavanje). Ako nema: recite neprovjereno i što bi to potvrdilo.

3) Stupanj i učinak (brzo). Širi li se izvan niše? Tko je meta? Jesu li vidljivi neki lanci geoblokiranja/preusmjeravanja/oglasa? Zabilježite ako dodiruje poznate ranjivosti zajednice.

4) Mikro-pisanje. Dvije rečenice: ono što se tvrdi; ono što ste pronašli (s najjačom vezom). Jedna rečenica: povjerenje + razlog („najraniji primjer iz 2019. pokazuje drugačiji kontekst"; „nema zapisa u primarnom skupu podataka"). Etička provjera: izbjegavajte širenje laži u naslovu; ne uključujte nepotrebne osobne podatke.

Rezultati:

- Zaključak od 1 odlomka (Istinito / Netočno / Obmanjujuće / Neprovjereno) s povjerenjem.
- 3 poveznice (podrijetlo, najbolja alternativna pokrivenost, primarna/službena).
- Oznake odgovora: tiho pojašnjenje / kratka javna objava / povećati na 30-minutnu provjeru.

Uobičajene zamke koje treba izbjegavati: emocionalno nabijeno predstavljanje, statistika bez izvora, web stranice „profesionalnog izgleda“, ali maskirane i propagandne taktike usmjerene na identitet.

30 minuta — Potpuna provjera (ponovljivo, spremno za javnost)

Cilj: Transparentno, arhivirano objašnjenje s proporcionalnim smjernicama za odgovor.

0) Administracija i sigurnost. Započnite bilješku (datum, tim, nadzirani kanali). Arhivirajte sve ključne URL-ove (Wayback/Perma). Ako postoji rizik od uznemiravanja ili „doxxinga“, prijeđite na sigurniju komunikaciju; zabilježite incidente (obveza zaštite).

1) Karta ABCDE. Akter: Tko stvara i širi? Ima li znakova državnih medija, farmi lažnih identiteta, plaćenih trolova, botneta, influencera? Provjerite legitimne novinare/medije putem službenih stranica (bez lažnog predstavljanja).

- Ponašanje: domene zlouporabe pogrešaka u tipkanju/klonirane domene, kopirani predlošci, lanci preusmjeravanja, plaćeni oglasi, geo-blokiranje, sinkronizirano objavljivanje, komentarske brigade, „preplavljivanje“ manipuliranim chatbotovima. Dokument sa snimkama zaslona + vremenske oznake.
- Sadržaj: Točne formulacije, vizualni elementi, uređivanja/izrezivanja, emocionalni znakovi, nedostajući kontekst. Usporedite s najranijim pojavljivanjima iz Lens/TinEye ili pretraživanjima ključnih kadrova.
- Stupanj: Doseg/brzina/publika; potražite način zarade; zabilježite uključene platforme.
- Učinak: Moguća šteta (javna sigurnost, građansko povjerenje, ugled). Odaberite učinkovit kanal s najmanjom mogućnošću širenja za odgovor.

2) Skup dokaza

- Primarni/službeni: skupovi podataka, pravni/agencijski dokumenti, zabilježene izjave.
- Neovisno izvještavanje/stručnjaci: renomirani mediji, priznati stručnjaci.
- Tehničke provjere: WHOIS/starost domene, TLS certifikati; C2PA/vjerodajnice sadržaja (ako postoje); EXIF/metapodaci (ako su dostupni); stil/vrijeme/vremenski uvjeti/obilježja koja provjeravaju geolokaciju (Street View/Mapillary, sunce/sjena).
- Elementi kampanje: predstavljanje s ciljem nanošenja štete, trolovi/botovi, manipulacija algoritmima, influenceri i maskerada časopisa/znanosti – uhvatite primjere.

3) Perspektiva ranjivosti. Obratite pažnju na kontekst: polarizacija, niska medijska pismenost, nejednakost, slaba kibernetička sigurnost, nisko povjerenje, slaba regulacija. Ako je više odgovora „da“, dajte prioritet savjetima o „prebunkingu“ + medijskoj pismenosti u odgovoru.

4) Analiza i zaključak. Napišite kratko objašnjenje sa:

- Naslovom koji se vodi istinom (ne laži).
- Sažetak s 3 točke (što je točno/netočno, što nedostaje, zašto je važno).
- Metoda (što ste provjerili, kako).
- Zaključak + pouzdanost (Istina / Laž / Obmanjujuća / Neprovjerena + Visoka / Srednja / Niska).
- Izvori i arhivi (podrijetlo, najjači dokazi, alternative).
- Proporcionalni odgovor (tiho informiranje / kratka javna korekcija s 1 mjerodavnom poveznicom / cjelovita objava + koordinacija koalicije / medijski zahtjev).
- Sigurnosna i etička napomena (poštuje se privatnost, nesigurnost je navedena, nema „doxxinga“).

5) Objavite i pratite. Odaberite kanal/e koji minimizira širenje (sadržaja), ali dopire do ciljane publike. Dodajte plan praćenja: tko prati koje platforme 48–72h; kada ažurirati/povući.

Predložak javnog objašnjenja

- Naslov: Vodite se provjerenom istinom (izbjegavajte ponavljanje lažne tvrdnje).
- Sažetak (3 točke): [A], [B], [C].
- Što smo provjerili: [Tvrdnja, gdje se pojavila, najraniji primjer].
- Kako smo provjerili: [Alati: Lens/TinEye/ključne sličice/WHOIS/skup podataka X].
- Što smo pronašli: [Sažeti narativ s poveznicama].
- Zaključak i povjerenje: [Npr. obmanjujuće — srednje povjerenje].
- Zašto je to važno: [Učinak na zajednicu/odluku].
- Izvori i arhiva: [url-ovi + arhivske poveznice].
- Napomene o ograničenjima i sljedećim koracima: [Što bi podiglo povjerenje].
- Kontakt: [NVO/AF komunikacijska adresa].

Alati i tehnike

Ovi alati i tehnike su praktični „kako“ našeg skupa alata – ponovljive metode koje skepticizam pretvaraju u pouzdanu verifikaciju. Oni pokrivaju cijeli luk (životni ciklus) tvrdnje: provenijenciju i razvrstavanje trijažu izvora; provjere slike, videozapisa i zvuka (uključujući znakove manipulacije umjetnom inteligencijom); verifikaciju citata i podataka; forenziku domena/web stranica za tipfelere i klonove; trijažu društvenih mreža; OSINT geo/krono-lokaciju; otkrivanje obrazaca kampanje koristeći ABCDE; leću ranjivosti za prilagodbu odgovora; te etiku, sigurnost i arhiviranje radi sljedivosti. Pružamo ih kako bi svaki ambasador mogao djelovati brzo i dosljedno, izbjeći slučajnu amplifikaciju (pojačavanje), proizvesti transparentne, reproducibilne nalaze i odabrati najmanje pojačavajući odgovor, a ipak uvijek štiti povjerenje naše zajednice.

Provenijencija i trijaža izvora

Kada koristiti: Prvi kontakt s bilo kojom tvrdnjom.

Kako: Provjerite izdavača, dosadašnja postignuća, tvrdnju o stručnosti, financiranju i tko je tu tvrdnju pojačao. Otvorite neovisne kartice (lateralno čitanje) i usporedite domenu sa službenom stranicom medija kako biste uhvatili lažno predstavljanje i „typosquatove“ (stranice slične originalu).

Rezultati: Ocjena izvora u jednom retku + poveznica na službenu stranicu za kontakt/informacije „o nama“.

Zamke: Kredibilitet postignut dizajnom (profesionalnog izgleda, ali lažan), pozivanje na autoritet bez provjerljivih vjerodajnica.

Vizualna provjera (slike)

Kada koristiti: fotografije, snimke zaslona, memeovi, „slike s dokazima“.

Kako: spremite datoteku → pokrenite Google Lens i TinEye → pronađite najranija pojavljivanja i podudaranja veće razlučivosti → provjerite ima li izrezivanja/uređivanja ili ponovno korištenih slika u novim kontekstima.

Rezultati: URL adresa najranijeg podudaranja + datum, 1–2 poveznice (linka) za usporedbu, zaključak (izvorno/uređeno/ponovno korišteno).

Zamke: Oslanjanje na jedan alat; ignoriranje jezičnih/regionalnih filtera; zaboravljanje arhiviranja.

Provjera videozapisa i zvuka (uključujući AI znakove)

Kada koristiti: isječci, reelovi, govori, glasovne bilješke.

Kako: izdvojite 3 – 5 ključnih kadrova → obrnutom pretragom pretražite svaki; usporedite zvuk i pokrete usta; poslušajte ima li pretjerano čiste, monotone boje glasa. Koristite popis znakova AI - videozapisa: neusklađenost usana i govora, A/V desinkronizacija (neusklađenost zvuka i slike), staklasti pogled/bez treptanja, previše glatka koža, deformirane ruke/prsti, robotska izvedba (govor).

Rezultati: podudaranja ključnih kadrova, kratka bilješka o dosljednosti A/V, zaključak + pouzdanost.

Zamke: Suđenje po „vibri"; ignoriranje akustike prostorije/neusklađenosti osvjetljenja; zaboravljanje da pravi video niske kvalitete može izgledati „AI-ovski".

Provjera citata/tvrdnji

Kada koristiti: „X je rekao Y", viralne snimke zaslona objava, naslova.

Kako: pretražite točnu frazu u citatima, provjerite službene kanale (stranice za tisak, provjerene račune), usporedite vremenske oznake. Za snimke zaslona potražite izvorni post ili arhiviranu kopiju prije nego što vjerujete izrezanoj slici.

Rezultati: Poveznica na izvorno ili autoritativno opovrgavanje/potvrdu; zaključak + razina pouzdanosti.

Zamke: Lažne snimke zaslona; satira izvan konteksta; fragmenti citata koji preokreću značenje.

Podaci, brojevi i grafikoni

Kada koristiti: Ankete, statistika kriminala, zdravstveni brojevi, „studija pokazuje".

Kako: Identificirajte primarni skup podataka; provjerite vremenski okvir, metodu, nazivnike i isključenja; ponovno izračunajte jednostavnu provjeru ako je moguće. Zabilježite nesigurnost i marginu pogreške.

Rezultati: Poveznica na primarni izvor, metoda bilješke u jednoj rečenici, ispravljena slika (ako je potrebno).

Zamke: Proizvoljno odabrani rasponi, postotak naspram postotnih bodova, projekcije modela tretirane kao opažanja.

Forenzika web stranica i domena

Kada koristiti: Sumnjivi klonirani mediji/stranice, „typosquatovi" (stranice slične originalu), lanci preusmjeravanja.

Kako: Usporedite pravopis domene i TLD sa stvarnim medijem; provjerite WHOIS/datum izrade, TLS certifikat, potpise autora i „slugove" sekcija; slijedite poveznice da vidite petljaju li se putem preusmjerivača ili geo-blokiranih ruta. Zabilježite oglase koji se prikazuju samo na klonu (signal ponašanja).

Rezultati: Usporedne činjenice o domeni (starost/izdavatelj/putanje), snimke zaslona izgleda/potpisa autora, zaključak (legitimno/klonirano).

Zamke: Pretpostavka da HTTPS podrazumijeva autentičnost; nedostaju suptilne zamjene domena (rn vs. m).

Trijaža društvenih mreža

Kada koristiti: Računi, teme, popularni postovi.

Kako: Arhivirajte objavu; skenirajte povijest računa u potrazi za „copy-paste“ nizovima, obrascima vremenskih zona, iznenadnim skokovima pratitelja ili identičnim nizovima komentara (botovi/brigade). Provjerite koreografiju „hashtagova“ i unakrsno objavljivanje na drugim platformama.

Rezultati: 3–5 snimaka zaslona s vremenskim oznakama; bilješka o koordinacijskim signalima; brza procjena stupnja (doseg/brzina).

Zamke: Pretjerano pripisivanje koordinacije fandomima (zajednicama obožavatelja); ignoriranje jezičnih varijanti.

OSINT geolokacija i kronolokacija

Kada koristiti: "Ovo se dogodilo ovdje/sada" tvrdnje.

Kako: Usporedite orijentire putem Google Maps/Street View/Mapillary/OpenStreetMap; usporedite horizonte, urbanu opremu, znakove trgovina. Procijenite vrijeme pomoću smjera sunca/sjene, vremenskih arhiva ili kalendara događaja.

Rezultati: Usklađene koordinate + slike dokaza; procjena vremena (ako je izvedivo).

Zamke: Obnovljeni/novi natpisi od snimanja slika; zrcalni/izrezani vizuali.

Otkrivanje obrazaca kampanje (povezano s ABCDE-om)

Kada koristiti: ponavljajući narativi ili plasiranje sadržaja putem više vrsta medija.

Kako: Zabilježite Aktera (mediji usklađeni s državom, farme persona, influenceri), Ponašanje (e-mailovi lažnog predstavljanja, „tiposquatovi“, klonirani izgledi, oglasi, lanci preusmjeravanja, geo-blokiranje), Sadržaj (identične točke razgovora), Stupanj (širenje na više platformi), Učinak (ciljana publika, vjerojatna šteta).

Rezultati: Obrazac na jednoj stranici + preporuka proporcionalnog odgovora.

Zamke: Tretiranje jednog posta kao problema kada je infrastruktura poanta.

Leća ranjivosti (kontekstno osjetljiv rizik)

Kada koristiti: Prije objavljivanja ili uključivanja zajednica.

Kako: Pokreni kontrolni popis: polarizacija, razina medijske pismenosti, socioekonomska nejednakost, slaba kibernetička sigurnost, nisko povjerenje u institucije, slaba regulacija. Ako je nekoliko odgovora "da", preferirajte prebunk (preventivno razotkrivanje), pažljiv ton i lokalne glasnike.

Rezultati: kontekstna bilješka u 2 retka koja opravdava odabir odgovora.

Zamke: Okrivljavanje publike; ignoriranje nositelja znanja u zajednici.

Etika, sigurnost i usklađenost

Kada koristiti: Svaka provjera prije objave.

Kako: Primijenite etičku provjeru: minimizirajte štetu, izbjegavajte nepotrebne osobne podatke, pokažite nesigurnost, koristite kanal s najmanjim pojačavanjem (amplificiranjem), zabilježite uznemiravanje i prijavite ga ako je potrebno, poštujte autorska prava/pristanak/GDPR.

Rezultati: Zapisnik s kućicama za označavanje u spisu predmeta.

Zamke: Ponavljanje laži u naslovima; slučajni „doxxing“ (snimke zaslona s osobnim podacima).

Arhiviranje i sljedivost

Kada koristiti: od prvog klika.

Kako: Spremite izvorne URL-ove, snimke zaslona s vremenskim oznakama i arhivske kopije (Wayback/Perma). Dosljedno imenujte datoteke. Vodite kratki dnevnik metoda kako bi kolega mogao reproducirati vaš rezultat.

Rezultati: Kompaktna mapa predmeta (podrijetlo → metoda → zaključak).

Zamke: Pokretne mete (izbrisani postovi); nedostajuće vremenske zone.

Europske studije slučaja

Ove europske studije slučaja su konkretni scenariji iz stvarnog svijeta – poput kloniranih medija operacije Doppelgänger, rekonstrukcije OSINT-a MH17, predizbornog deepfake zvuka u Slovačkoj, deepfake-a „predaje“ Zelenskog i litvanske hibridne operacije uz korištenje botova i prevara – koji omogućuju ambasadorima da vježbaju točne vještine iz našeg skupa alata u uvjerljivim uvjetima. Svaki od njih spaja narativ s točnim signalima, alatima i radnim procesima koje podučavate (SIFT • 10-minutna provjera • 30-minutni ABCDE) i oslanja se na praksu u stilu Debunka (razotkrivanje lažnih informacija). Uključujemo ih kako bismo apstraktne metode pretvorili u mišićnu memoriju: uočavanje signala ponašanja (klonirane domene, preusmjeravanja, botovi), izvođenje brzih vizualnih/audio provjera (Lens, TinEye, ključni kadrovi, AI-tells), mapiranje ABCDE-a za odabir proporcionalnog odgovora i dokumentiranje nalaza s arhivama i oznakama pouzdanosti. Vježbajući s europskim primjerima bliskim našem kontekstu, timovi uče brzo djelovati, izbjegavati slučajno pojačavanje (amplificiranje) i štititi povjerenje zajednice transparentnom, ponovljivom verifikacijom.

"Operacija Doppelgänger" – klonirani mediji i „typosquatovi“ usmjereni na EU

Narativ. Dugotrajna operacija utjecaja objavljuje članke na domenama sličnog izgleda koje oponašaju europske medije i institucije, a zatim ih pojačava putem oglasa, preusmjeravanja i odabira influencera.

Signali i alati. Forenzika domene (tipfeleri/zamjene TLD-a, starost WHOIS-a, izdavatelj TLS-a), nepodudarnosti izgleda/podnaslova/stranica za kontakt; lanci oglasa/preusmjeravanja; geo-blokiranje; arhiviranje.

Mapiranje radnog procesa. SIFT (uočavanje lažnog predstavljanja); 10-min (domena/TLS + najranija pojavljivanja slika putem Lensa/TinEyea); 30-minutni ABCDE (Akter = infrastruktura + pojačanje (amplifikacija); Ponašanje = klonovi/oglasi/preusmjeravanja; Stupanj = širenje na više platformi; Učinak = reputacijska/građanska šteta).

Što podučavati. "Podrijetlo na prvom mjestu", a zatim brzi komentari; tretirajte infrastrukturu (mrežu klonova) kao priču, a ne samo jedan post.

Čitaj više. pregledi i PDF-ovi EU DisinfoLaba; CORRECTIV-ova analiza usmjeravanja lanca preusmjeravanja.

MH17 (2014) — OSINT geolokacija i rekonstrukcija vremenske trake

Narativ. Konkurentske tvrdnje uslijedile su nakon obaranja leta MH17 iznad istočne Ukrajine. Istražitelji otvorenih izvora (OSINT) ušli su u trag ruti lansera Buk, povezujući slike, serijske oznake, putokaze i vremenske oznake.

Signali i alati. Obrnute provjere slika/videozapisa, Street View/Mapillary, podudaranje natpisa/orijentira, provjere sjena/vremena, snimke arhiva; strukturirana bilježnica slučaja (bilješke).

Mapiranje radnog procesa. 10-minutno (ključni kadrovi → obrnuto pretraživanje; triangulacija najranijih objava); 30-minutni ABCDE + skup dokaza (primarni/službeni nalazi, ugledno izvještavanje, OSINT).

Što podučavati. Kako metode koje se mogu reproducirati i arhiviranje stvaraju pouzdanost na razini sudnice.

Čitaj više. Bellingcatovo izvješće(a); kasnije reference u europskim postupcima i medijima.

Slovačka 2023. – predizborni deepfake audiozapisa

Narativ. Nekoliko dana prije glasanja (tijekom medijske šutnje) pojavio se zvuk generiran umjetnom inteligencijom, predstavljajući se kao razgovor o namještanju izbora, koji se brzo širio na društvenim platformama i aplikacijama za razmjenu poruka.

Signali i alati. Osnove audio forenzike (ton sobe, rezovi, prozodija); praznine u izvoru/provenijenciji; iznenadno podizanje na više platformi; pojačavanje od strane influencera bez primarnog izvora; slijepe točke (mane) platformskih pravila za zvuk.

Mapiranje radnog procesa. SIFT (ne amplificirajte; snimajte originale; zabilježite rizik od razdoblja šutnje); 10 minuta (pretraživanje točne fraze; tražite originalnu objavu; usporedite s provjerenim uzorcima glasa; bilježite nesigurnost); 30 minuta (opseg i učinak → proporcionalan odgovor; smjernice za „prebunking“ za partnere).

Što podučavati. Zašto je audio deepfake sadržaj teže kontrolirati nego video sadržaj – i kako jasno i brzo komunicirati nesigurnost.

Čitaj više. Wired objašnjenje; Bloombergovo izvještavanje; baze podataka incidenata koje sažimaju plasiranje (audiozapisa) i vremenski raspored.

Zelenski „surrender“ deepfake (2022.) — brzo razotkrivanje u ratno vrijeme

Narativ. Lažni videozapis predsjednika Zelenskog koji poziva na predaju nakratko je emitiran na internetu (i navodno putem kompromitiranih medija), ali mu je brzo uzvraćeno autentičnom izjavom i uklanjanjem sadržaja s platformi.

Signali i alati. AI-video govori: neusklađenost usana/AV-a, staklasti pogled, preglatka koža; obrnuto pretraživanje ključnih kadrova; provjere podrijetla; provjera službenog kanala.

Mapiranje radnog procesa. 10-minutno (ključni kadrovi → obrnuto pretraživanje; zapis o sinkronizaciji A/V-a; provjeriti na službenim kanalima); 30 min (jasno objašnjenje koje se vodi istinom; arhivske poveznice; oznaka pouzdanosti).

Što podučavati. Spremnost + brze poruke koje su na prvom mjestu istinite mogu ublažiti utjecaj čak i kada deepfake dospije u javnost.

Čitaj više. France24 razotkrivanje; kontekst Euronewsa; analiza priručnika za brzu protuporuku.

Litva (2023.–2024.) – hibridna prijevara velikih razmjera + širenje dezinformacija

Narativ. Debunk.org je dokumentirao koordinirani napad koji miješa stranice za prevaru, neautentične račune i prokremljanske narative usmjerene na litvansku publiku; kasnija izvješća prate mreže botova i tematske kampanje (npr. sadržaj vezan uz Kalinjingrad).

Signali i alati. Mrežni signali („copy-paste“ nizovi, obrasci vremenskih zona), aktivnost slična botovima, brendiranje kampanje, unakrsno objavljivanje; provenijencija + arhiviranje; leća ranjivosti (niska razina povjerenja, regionalne napetosti).

Mapiranje radnog procesa. SIFT (arhiva; trijaža izvora); 10 min (povijest računa; provjere na više platformi; najranija pojavljivanja); 30-minutna ABCDE (Akter/Ponašanje = bot mreže + trolovske stranice; Opseg = doseg/brzina; Učinak = rizik zajednice) → matrica odgovora i „prebunking“.

Što podučavati. Spojite točke iz objava → mreže → narativa → štete, zatim odaberite najmanje pojačavajući učinkovit odgovor.

Čitaj više. Istrage Debunk.org-a i daljnje analize o mrežama botova i ciljanim temama.

Priručnik za zemlju

Svrha ovih priručnika za zemlje je lokalizirati metode, izvore i primjere za svaki ciljani kontekst. Odabrali smo zemlje u kojima su provedene aktivnosti ovog projekta - Austriju, Hrvatsku i Litvu.

Svaki priručnik uključuje 10 najboljih vjerodostojnijih izvora (vladini/agencijski podatkovni portali; partneri za provjeru činjenica), uobičajene narative i sezonske cikluse (npr. izbori, energija, migracije, javno zdravstvo), obrasce lokalnih platformi (aplikacije za razmjenu poruka naspram otvorenih mreža; jezične varijante), pravne specifičnosti/specifičnosti usklađenosti (podaci, mediji, prozori za izbornu šutnju) i tri lokalne vinjete slučajeva sa spremnim vježbama.

Litva (LT)

Najbolji vjerodostojni izvori (za brzo povezivanje):

- Službena statistika: Statistički zavod Litve / Državna agencija za podatke (portal OSP) – www.osp.stat.gov.lt
- Izbori: Središnje izborno povjerenstvo (VRK). – www.vrk.lt
- Zdravstvo: Ministarstvo zdravlja (SAM) - www.sam.lrv.lt
- Kibernetička sigurnost: Nacionalni centar za kibernetičku sigurnost (NCSC) – www.nksc.lt
- Provjera činjenica/OSINT reference: Debunk.org (regionalne analize) – www.debunk.org

Uobičajeni narativi i sezonski ciklusi: granični/migracijski incidenti; energetski/cjenovni šokovi; prisutnost NATO-a; glasine u izbornom razdoblju; strahovi povezani sa zdravstvenom politikom. Koristite „prebunk“ predloške kada kalendari VRK-a objave ključne točke.

Točke praćenja i obrasci platformi: klonirane medijske domene i članci u stilu Doppelgängera; geo-blokirana preusmjeravanja; unakrsno objavljivanje na Facebooku/Telegramu. Pokrenite provjere domene/TLS-a/WHOIS-a + obrnutu pretragu sliku (Lens/TinEye) za ponovno korištene vizualne elemente.

Pravne napomene/napomene o usklađenosti: provjerite stranice VRK-a za trenutne informacije o izborima prije objavljivanja ispravaka; arhivirajte (Wayback/Perma) sve poveznice korištene u provjeri.

Hrvatska (HR)

Najbolji vjerodostojni izvori:

- Službena statistika: Državni zavod za statistiku (DZS) – www.dzs.gov.hr
- Izbori: Državno izborno povjerenstvo (DIP/SEC) - www.izbori.hr

- Zdravstvo: Ministarstvo zdravstva – www.zdravlje.gov.hr
- Kibernetička sigurnost: Nacionalni CERT (CERT.hr / CARNET) - www.CERT.hr

Uobičajeni narativi i sezonski ciklusi: teme EU-a (Schengen/euro), migracijske rute, energija/turizam, glasine u izbornoj sezoni. Očekujte copy-paste navale na Facebook stranicama i portalima.

Točke praćenja i obrasci platformi: tipfeleri nacionalnih medija; Telegram/FB grupe recikliraju stare fotografije s novim natpisima. Koristite 10-minutni tijek: ključne kadrove → obrnuto pretraživanje; provjera starosti domene/TLS-a.

Pravne napomene/napomene o usklađenosti: koristite stranice SEC-a za postupke i vremenske rokove kada se zahtjevi odnose na glasovanje ili izlaznost; arhivirajte snimke zaslona s vremenskim oznakama u slučaju da se objave izbrišu.

Austrija (AT)

Najbolji vjerodostojni izvori:

- Službena statistika: STATISTIKA AUSTRIJE - www.statistik.at
- Izbori: Savezno izborno povjerenstvo (Bundeswahlbehörde) putem Ministarstva unutarnjih poslova - www.bmi.gv.at
- Zdravstvo: Savezno ministarstvo socijalne skrbi, zdravstva, skrbi i zaštite potrošača. - www.sozialministerium.gv.at
- Kibernetička sigurnost: CERT.at (nacionalni CERT) – www.cert.at

Uobičajeni narativi i sezonski ciklusi: cijene energije i klimatska politika; EU regulativa; migracije; prekogranične priče s Njemačkom (DE), Italijom (IT) i Češkom (CZ). Klonirane stranice ponekad oponašaju ministarstva ili nacionalne televizijske kuće.

Točke praćenja i obrasci platforme: lanci preusmjeravanja i položaji oglasa na sličnim stranicama s vijestima; lokalne Facebook grupe koje dijele snimke zaslona s njemačkih stranica. Prvo potvrdite provenijenciju (podrijetlo); mapirajte ponašanje (klonovi/oglasi/preusmjeravanja) prije rasprave o sadržaju.

Pravne napomene/napomene o usklađenosti: informacije o izborima su centralizirane – povežite se na stranice Bundeswahlbehörde-a za pravila i službene obavijesti.

Zaključak

Ovaj skup alata pretvara dobre namjere u pouzdanu praksu. Kombiniranjem jasnih koncepata s radnim procesima 5/10/30, ABCDE trijažom te disciplinirano etikom i rutinom arhiviranja, svakom ambasadoru dajemo ponovljiv put od „ovo izgleda sumnjivo“ do transparentnog, proporcionalnog odgovora. Alati i tehnike – trijaža izvora, vizualna i audio provjera, forenzika domene, OSINT geo/krono provjere i otkrivanje obrazaca kampanje – namjerno su jednostavni za početak i dovoljno rigorozni da izdrže u javnosti. Europske studije slučaja, priručnici za zemlje i brze kartice prevode metode u mišićnu memoriju tako da timovi mogu djelovati brzo bez pojačavanja štete.

Najvažnije su dosljednost i pažnja. Predvodite istinom, pokažite svoju metodu i neizvjesnost i odaberite kanal koji najmanje pojačava, a koji još uvijek štiti ljude. Snimite originale, arhivirajte veze (linkove) i ostavite trag koji kolega može reproducirati sutra. Koristite leću ranjivosti za oblikovanje tona i vremena (tajminga); primijenite matricu odgovora kako bi se mjere uskladile s rizikom; i mjerite ono što radite s laganim KPI-jevima kako bi se kvaliteta poboljšala iz mjeseca u mjesec. Kako se platforme, taktike i umjetna inteligencija razvijaju i ovaj skup alata dizajniran je da se razvija: dodajte nove slučajeve, ažurirajte svoje brze kartice, osvježite listove zemalja i pokrenite redovite vježbe. Ako nastavimo učiti zajedno – i održavamo naš rad sljedivim, poštovanim i jasnim – jačamo povjerenje u našim zajednicama i otežavamo uspjeh manipulacije.

Prilozi

Pojmovnik

ABCDE okvir — Akter, Ponašanje, Sadržaj, Stupanj, Učinak — strukturirani način analize operacija.
Primjer: mapirajte mrežu (akter), koordinaciju (ponašanje), narative (sadržaj), doseg (stupanj) i utjecaj (učinak).

Arhiviranje (Wayback, Memento) — Spremanje snimaka web stranica radi očuvanja dokaza i usporedbe promjena.
Primjer: Wayback pokazuje da je naslov uređen nakon objave.

Atribucija — Procjena tko vjerojatno stoji iza operacije; često ukinuta i utemeljena na dokazima.
Primjer: Jezični obrasci i hosting povezuju web-lokaciju s poznatom tvrtkom za utjecaj.

Bias (Pristranost) i heuristika — Kognitivni prečaci (potvrda, dostupnost, motivirano rasuđivanje) koji iskrivljuju prosudbu.
Primjer: Poželjno primjećujete primjere koji odgovaraju vašim prethodnim uvjerenjima.

Bot / Automatizacija — Računi koji automatski objavljuju ili pojačavaju sadržaj neprirodnom brzinom/razmjerom.
Primjer: profil objavljuje svake 2 minute, 24/7, na više jezika.

Lanac dokazivanja — Dokumentiranje načina na koji su dokazi pribavljeni i pohranjeni radi održavanja integriteta.
Primjer: bilježenje vremena preuzimanja, URL-a i hasha za videozapis.

Kronolokacija — Potvrda kada je slika/videozapis snimljen pomoću položaja sunca, vremenskih uvjeta ili tragova događaja.
Primjer: kutovi sjene i arhiva vremenskih uvjeta pokazuju da je videozapis iz travnja 2023.

Tvrdnja — Izjava koja tvrdi da je nešto istinito ili netočno; jedinica koju provjeravate.
Primjer: U objavi piše: "Grad je zabranio sve plinske peći od siječnja 2026."

Kolaps konteksta — Kada se informacija dijeli izvan izvornog konteksta, mijenja se njezino značenje.
Primjer: satirični naslov ponovno objavljen kao da je prava vijest.

Koordinirano neautentično ponašanje (CIB) – Organizirana upotreba lažnih računa/stranica za zavaravanje identiteta ili svrhe.
Primjer: skupina stranica svakodnevno dijeli identične postove u istoj minuti.

Ispravak / Ažuriranje — Transparentna bilješka koja ispravlja pogreške ili dodaje nove informacije nakon objave.
Primjer: "Ažurirano 4. studenog 2025.: ispravljen datum od 12. listopada do 21. listopada."

Unakrsno upućivanje — Potvrđivanje činjenice neovisnim, vjerodostojnim izvorima.
Primjer: Potvrđivanje brojeva putem službenog skupa podataka i zasebnog revizorskog izvješća.

Deepfake / sintetički mediji — Audio, slika ili video generiran ili izmijenjen umjetnom inteligencijom kako bi realno oponašao stvarne ljude ili događaje.
Primjer: glasovna snimka klonirana umjetnom inteligencijom koja lažno „priznaje“ zločin.

Dezinformacije – lažne ili obmanjujuće informacije koje su namjerno stvorene ili širene radi obmane.
Primjer: Mreža stranica krivotvori rezultate anketa kako bi obeshrabrila glasovanje.

DSA(Akt o digitalnim uslugama)/Kodeks ponašanja – Akt o digitalnim uslugama EU-a i dobrovoljni Kodeks kojim se usmjerava odgovornost i transparentnost platformi.
Primjer: platforme objavljuju biblioteke oglasa i procjene rizika po DSA-u.

Dokazi – Informacije koje podupiru ili opovrgavaju tvrdnju. Mogu biti dokumenti, podaci, slike, video ili svjedočenja stručnjaka.
Primjer: zapisnik glasovanja gradskog vijeća i službeni tekst pravilnika.

Geolokacija – Potvrda mjesta snimanja slike/videozapisa odgovarajućim orijentirima, znakovima ili terenom.
Primjer: prepoznavanje horizonta i uličnih znakova za postavljanje videozapisa u Kaunasu.

Hash / Kontrolna suma— Jedinstveni digitalni otisak prsta datoteke koji dokazuje da se nije promijenila.
Primjer: MD5/SHA256 podudara se prije i poslije prijenosa.

Lateralno čitanje — Otvaranje novih kartica kako bi se provjerilo tko je izvor prije pažljivog čitanja.
Primjer: najprije provjerite na stranici „O nama“ i vanjske profile.

Malinformacije — Istinite informacije koje se dijele izvan konteksta ili sa štetnim okvirom kako bi se nanijela šteta.
Primjer: curenje kućne adrese osobe radi poticanja uznemiravanja.

Metapodaci / EXIF — ugrađeni tehnički podaci o datoteci (uređaj, vrijeme, GPS). Često su ogoljeni platformama.
Primjer: Izvorna fotografija prikazuje GPS koordinate i vrijeme snimanja.

Misinformacije — Lažne ili obmanjujuće informacije koje se dijele bez namjere obmane.
Primjer: Prijatelj dijeli zastarjelu kartu s pogrešnim zonama evakuacije.

Narativ nasuprot tvrdnji — Narativ je šira priča; tvrdnja je specifična izjava koja se može provjeriti.
Primjer: Narativ: „Izbori su namješteni.“ Tvrdnja: „10.000 mrtvih birača glasalo je u gradu X.“

OSINT (Obavještajna služba otvorenog koda) — Prikupljanje i analiza javno dostupnih podataka radi provjere činjenica.
Primjer: Korištenje registara tvrtki i alata za praćenje letova za potvrdu putovanja osobe.

Prebunking / Inokulacija — Podučavanje taktika manipulacije i protuargumenata prije nego što se ljudi susreću s njima.
Primjer: Lekcija o „lažnim dilemama“ smanjuje kasniju osjetljivost.

Primarni izvor — Izvorni materijal stvoren u vrijeme događaja ili izravno od strane subjekta.
Primjer: Pravilnik PDF na službenoj web stranici grada.

Propagandna sredstva — Klasične tehnike: etiketiranje, blještave generalizacije, prijenos, svjedočanstva, obični ljudi, gomilanje karata, efekt krda.
Primjer: u oglasu se upotrebljava „svjedočanstvo“ slavne osobe bez dokaza.

Proporcionalnost – usklađivanje snage vašeg zaključka s kvalitetom/kvantitetom dokaza.
Primjer: „Neprovjereno“ kada su izvori u sukobu; Izbjegavajte preuveličavanje tvrdnji.

Oznake pouzdanosti – Oznake platforme ili treće strane za medije (npr. javni medij, povezan s državom).
Primjer: videozapis prikazuje oznaku „medij pod državnom kontrolom“ ispod naziva kanala.

Obrnuto pretraživanje slika — Pronalaženje starijih ili izvornih verzija slike radi provjere podrijetla i konteksta.
Primjer: praćenje fotografije prosvjeda do događaja iz 2016., a ne do „danas“.

Procjena sigurnosti i štete – Procjena potencijalnih rizika (privatnost, doxing, retraumatizacija) prije objavljivanja.
Primjer: zamagljujete lica maloljetnika na snimkama prosvjeda.

Satira / parodija — Šaljiv ili preuveličan sadržaj koji oponaša stvarne vijesti ili ljude.
Primjer: web-stranica objavljuje lažni članak o lansiranju raketa „ravne Zemlje“.

Sekundarni izvor — Sažetak, analiza ili izvješće temeljeno na primarnim izvorima.
Primjer: novinski članak koji opisuje pravilnik i citira dužnosnike.

SIFT metoda — Stanite, istražite izvor, pronađite bolju pokrivenost, pratite izvornik.
Primjer: Prije retweetanja zaustavite se i pronađite izvorno priopćenje za javnost.

Sockpuppet (lažni mrežni identitet)/ Astroturfing (lažna podrška)— Lažni identiteti koji glume podršku građana.
Primjer: Tvrtka vodi stranice za građane na kojima hvali njezin proizvod i napada kritičare.

Transparentnost izvora — Jasne informacije o tome tko vodi web-mjesto/račun, financiranju, pravilima ispravaka i podacima za kontakt.
Primjer: Medij navodi svoj urednički tim i dnevnik ispravaka.

Sendvič s istinom — Komunikacijska taktika: iznesite istinu → demantirati mit → ponovno iznesite istinu s dokazima.
Primjer: "Cjepiva su sigurna i učinkovita. Viralna objava lažno tvrdi X. Evo podataka koji pokazuju sigurnost."

Tijek rada verifikacije (5/10/30) — Dubina trijaže na temelju raspoloživog vremena: 5 min brza provjera, 10 min dublja, 30 min potpuna.
Primjer: Za 5 minuta provjeravate naslov, izvor i izvornu vezu; u 30 se obratite stručnjacima.

Financira Europska unija. Međutim, iznesena stajališta i mišljenja samo su stajališta autora i ne odražavaju nužno stajališta Europske unije ili Europske izvršne agencije za obrazovanje i kulturu (EACEA). Ni Europska unija ni davatelj potpore ne mogu se smatrati odgovornima za njih.