TOOLKIT ZUR FAKTENPRÜFUNG

Vilnius,
November 2025

Ein konsolidierter Leitfaden zu Methoden, Tools und Ressourcen für eine effektive Faktenprüfung

ATEITININKŲ FEDERACIJA, LITAUEN
PROJEKT DECIDE

Co-funded by the
European Union

Inhaltsverzeichnis

Einleitung 2
Grundlagen & Schlüsselkonzepte 6
Mit dem Faktencheck beginnen 10
Arbeitsabläufe 16
Werkzeuge und Techniken 21
Europäische Fallstudien 25
Länder-Playbooks 28
Schlussfolgerung 30
Anhänge 31

u ime obitelji
World Youth Alliance Southeast Europe
PLATTFORM CHRISTDEMOKRATIE
ATEITININKAI

Co-funded by the European Union

Einleitung

Über das Fact-Checking Ambassadors-Programm

Faktenprüfung ist der Prozess, bei dem überprüft wird, ob eine Behauptung, ein Bild, eine Statistik oder eine Geschichte korrekt ist. Es bedeutet, Informationen auf glaubwürdige Primärquellen zurückzuführen, den Kontext zu überprüfen und klar zu kennzeichnen, was wahr, falsch, irreführend oder unbewiesen ist – mit transparenten Beweisen.

Warum ist das heute so wichtig?

Informationsflut: Wir sind täglich Tausenden von Beiträgen ausgesetzt; Unwahrheiten verbreiten sich schneller als Korrekturen.

KI-generierte Inhalte: Deepfakes und synthetischer Text lassen Fakes überzeugend aussehen.

Entscheidungen mit hohem Einsatz: Schlechte Informationen können Wahlen, Gesundheitsentscheidungen und die öffentliche Sicherheit beeinflussen.

Vertrauen und Verantwortlichkeit: Eine rigorose Überprüfung stellt das Vertrauen in Institutionen und Medien wieder her.

Bürgerliche Widerstandsfähigkeit: Eine faktenkundige Öffentlichkeit ist schwerer zu manipulieren.

Das Fact-Checking Ambassadors Programme wurde ins Leben gerufen, um die Medienkompetenz, das kritische Denken und die zivilgesellschaftliche Widerstandsfähigkeit in ganz Europa zu stärken. Es bietet einen strukturierten und dennoch anpassungsfähigen Rahmen, der den Teilnehmern hilft, genaue Informationen zu erkennen, zu überprüfen und verantwortungsbewusst zu kommunizieren. Die Methodik identifiziert neun Leitlinien und setzt diese durch vier integrierte Umsetzungsteile um.

Dieses Material wurde anhand von Material zusammengestellt, das während einer Live-Veranstaltung mit dem Titel "Media Literacy Workshop: How to recognize and Combat Disinformation" vorgestellt wurde, die vom 10. bis 12. Oktober 2025 in Vilnius, Litauen, stattfand, und auf der Grundlage der Empfehlungen der Referenten durch öffentliche Informationsquellen ergänzt. Für die Verarbeitung der Informationen wurden KI-Tools eingesetzt.

Wir danken Prof. Dr. Darius Pilkynas und Assoc. Prof. Liutauras Ulevičius von der Fakultät für Kommunikation der Universität Vilnius, Jovita Tautkevičiūtė-Kalinauskienė vom Projekt Debunk.org für das zur Verfügung gestellte theoretische Material und Arnas Jasinskas von der Federation of Futures für die Durchführung eines lebhaften Seminars zum Thema Desinformation, deren Erkenntnisse auch bei der Erstellung dieses Toolkits nützlich waren.

Vision

Die Hauptvision des Fact-Checking Ambassadors-Programms besteht darin, vertrauenswürdige Community-Mitglieder in die Lage zu versetzen, Fakten zu erkennen, zu überprüfen und verantwortungsvoll zu kommunizieren – damit die Communitys widerstandsfähiger gegen Fehl- und Desinformationen werden und bessere Entscheidungen treffen können.

Ziele des Programms

Wissen: Die Teilnehmer können Fehl-/Desinformation/Propaganda definieren; gängige Taktiken beschreiben; Erklären Sie die Grundlagen von ABCDE und OSINT.

Fähigkeiten: Die Teilnehmer können eine 5-10-minütige Triage durchführen, Bilder/Videos/Texte verifizieren und eine transparente Argumentationskette dokumentieren.

Einstellungen: Die Teilnehmer gehen respektvoll um, vermeiden Konfrontationen und legen Wert auf Klarheit, Empathie und Genauigkeit.

Übung: Jeder Teilnehmer erstellt einen kurzen Faktencheck und einen Outreach-Aktionsplan, der auf seine Community zugeschnitten ist.

Multiplikation: Mindestens ein lokales Mikrotraining (60–90 Minuten), das innerhalb von 60 Tagen nach der Zertifizierung durchgeführt wird.

Wofür dieses Toolkit gedacht ist

Dieses Toolkit hilft den Botschaftern, kritisches Denken in eine konsequente tägliche Praxis umzusetzen: wie sie fragwürdige Behauptungen erkennen, sie effizient überprüfen und Ergebnisse verantwortungsvoll innerhalb Ihrer NGO und der breiteren Gemeinschaften kommunizieren können. Es geht zuerst um die Aufgabe: kurze Erklärungen, dann konkrete Maßnahmen, die Sie in 5/10/30 Minuten ergreifen können, plus Beispiele und Arbeitsblätter. Lesen Sie es einmal, um die Karte zu lernen, und kehren Sie dann zurück, wenn Sie Schulungen planen, auf Vorfälle reagieren oder neue Botschafter betreuen. Behandeln Sie es als praktisches Feldhandbuch, nicht als Theorielektüre, und stützen Sie sich auf die Quick Cards und Links. Das Ergebnis ist eine gemeinsame Sprache, klare Arbeitsabläufe und eine Grundlage für Qualität.

Sie werden es für folgende Zwecke verwenden:

Bewerten Sie Behauptungen und Quellen schnell, auch unter Zeitdruck.

Wählen Sie die richtigen Verifizierungstools und Workflows.

Erklären Sie Ihre Argumentation klar und respektvoll gegenüber Nicht-Experten.

Unterstützen Sie die Kommunikation Ihrer NGO mit zuverlässigen, dokumentierten Kontrollen.

Was ist in diesem Toolkit enthalten?

Das Toolkit verankert sich in klaren Konzepten – Fehlinformationen, Desinformationen und Malinformationen – und Gewohnheiten wie laterales Lesen und Provenienzprüfungen, Inokulation/Prebunking und rigorose Quellentriage, die alle darauf abzielen, jede Überprüfung reproduzierbar zu machen. Er stellt moderne Desinformation als ein schnelles, skalierbares System dar, in dem Aufmerksamkeitserfassung und Identitätshinweise wichtiger sind als Medium, und betont, dass transparente Verifizierungs-, Archivierungs- und Provenienzstandards nach wie vor der beste Hebel sind.

Eine praktische ABCDE-Linse verlagert die Arbeit von Post-by-Post-Reaktionen auf das Systembewusstsein: Akteur, Verhalten, Inhalt, Grad, Wirkung – wird verwendet, um zu entscheiden, ob/wo und wie stark eingegriffen werden soll. Der Abschnitt behandelt auch, warum Menschen Unwahrheiten glauben (Bestätigungs-/Verfügbarkeitsverzerrungen, motivierte Argumentation, klassische Propagandamittel) und fordert wahrheitsorientierte, respektvolle Botschaften, um Fehlschüsse zu vermeiden. Er erklärt die Rolle der KI sowohl bei der Erzeugung als auch bei der Verstärkung und schreibt Gegenmaßnahmen vor: Verifizierung der Herkunft, Verwendung von visueller/akustischer Forensik (Keyframes, Rückwärtssuche), Archivierung jedes Schritts und Kommunikation von Unsicherheiten.

Zeitlich begrenzte 5/10/30-Workflows setzen Theorie in wiederholbare Maßnahmen um. Die 5-minütige SIFT-Triage verhindert eine versehentliche Amplifikation; Der 10-minütige Ablauf führt zu einem kurzen Urteil mit einem Vertrauensetikett; Der 30-minütige Check dokumentiert ABCDE, Kontext, Ethik und eine proportionale Antwort mit einer öffentlich zugänglichen Erklärungsvorlage.

"Tools & Techniques" beschreiben die praktischen Anleitungen: Provenienz- und Quellen-Triage, Reverse-Image- und Keyframe-Suche, Zitat-/Nummernverifizierung, Domain-/Website-Forensik für Klone/Typosquats, Triage in sozialen Netzwerken, OSINT-Geo-/Chrono-Checks, Erkennung von Kampagnenmustern in Verbindung mit ABCDE, eine Schwachstellenlinse zur Anpassung von Antworten und strenge Archivierung/Rückverfolgbarkeit. Es enthält auch eine "Was wann zu verwenden ist" und eine Antwortmatrix, um den Grad × Effekts mit den am wenigsten verstärkenden Aktionen abzugleichen. Ethik- und Sorgfaltspflicht-Leitplanken – minimieren Sie Schäden, schützen Sie die Privatsphäre, zeigen Sie Unsicherheit und halten Sie Datenregeln ein – sowie eine Qualitätscheckliste machen die Ergebnisse sicherer und reproduzierbar.

Schließlich verwandeln europäische Fallbeispiele (z. B. Operation Doppelgänger, MH17, Deepfake-Audio in der Slowakei 2023, Selenskyj-Deepfake, LT-Hybrid-Pushes) Methoden in

einem Muskelgedächtnis durch 30-minütige Labore, die Verifizierung, ABCDE-Mapping und proportionale Reaktion kombinieren.

Grundlagen & Schlüsselkonzepte

Bevor Sie etwas überprüfen, ist es wichtig zu verstehen, mit welcher Art von Informationen Sie es zu tun haben. Klare Definitionen verhindern Verwirrung und halten Diskussionen produktiv. Verwenden Sie sie bei der Planung und Nachbesprechung und verknüpfen Sie die Begriffe in Ihren internen Dokumenten. Achten Sie auf häufige Verwechslungen wie Absicht (Irrtum vs. Desinformation) und die Vernachlässigung von Fehlinformationen. Jeder Eintrag sollte ein zweizeiliges Beispiel und einen "Siehe auch"-Link zu Methoden enthalten.

Arten von falschen oder irreführenden Informationen:

Fehlinformationen – falsch, aber ohne die Absicht geteilt, Schaden anzurichten.

Desinformation – falsche Inhalte, die mit der Absicht geteilt werden, zu täuschen.

Malinformationen – echte Informationen, die aus dem Zusammenhang gerissen werden, um Schaden anzurichten (z. B. Doxxing).

Weitere wichtige Konzepte:

Verifizierung vs. Validierung: Die Verifizierung prüft Fakten (was ist passiert?). Die Validierung prüft die Schlussfolgerung und die Methode (stützen die Beweise die Behauptung?).

Laterale Lektüre und Provenienz: Anstatt auf einer Seite zu bleiben, öffnen Sie neue Tabs, um zu überprüfen, wer die Quelle ist. Bevor Sie Inhalte ansprechen, sollten Sie herausfinden, wer/was/wo/wann/warum.

Inokulation / Prebunking: Menschen warnen, *bevor* sie auf Manipulationen stoßen. Kurze, proaktive Warnung + Beispiel für die Manipulationstechnik zum Aufbau von Resistenzen vor der Exposition.

Quellensichtung: wer hat veröffentlicht, Erfolgsbilanz, Referenzen/Anspruch auf Fachwissen, Finanzierung, wer hat geteilt.

Gesellschaftliche Schwachstellen: Polarisierung, geringe Medienkompetenz, Ungleichheit, schwache Cybersicherheit, geringes institutionelles Vertrauen, schwache Plattformregulierung → höheres FIMI-Risiko.

Nachvollziehbarkeit: Jede Behauptung, die Sie veröffentlichen, muss von einem Kollegen anhand Ihrer Notizen, Links und archivierten Erfassungen reproduzierbar sein.

Im Glossar finden Sie prägnante Definitionen und Beispiele.

Co-funded by the European Union

Eine kurze Geschichte der modernen Desinformation

Vordigitale Wurzeln (spätes 19.–mittleres 20. Jh.). Lange vor dem Internet lernten Staaten und politische Bewegungen, Gerüchte, gefälschte Dokumente und Massenmedien als Waffe einzusetzen. In den frühen 1900er Jahren wurde in Zeitungen und Plakaten Propaganda in industriellem Maßstab verbreitet; Der Erste und der Zweite Weltkrieg professionalisierten Techniken wie emotionales Framing, selektive Statistiken und die Dämonisierung von Fremdgruppen. Radio und Wochenschauen senkten die Verbreitungskosten und erhöhten den Einsatz: Wenn man einen Sendeturm erobern konnte, konnte man die Realität für eine Nation über Nacht gestalten. Diese Perioden lehren zwei bleibende Lektionen: Medien ändern sich, aber psychologische Hebel – Angst, Identität, Groll – sind bemerkenswert stabil; Und Verteilungssteuerung ist Macht.

Die "aktiven Maßnahmen" des Kalten Krieges (1945–1991). Die Dienste der Sowjetunion und des Warschauer Pakts führten mehrjährige Beeinflussungskampagnen durch, bei denen Fälschungen, Tarnungen und erfundene Geschichten vermischt wurden. Die berühmteste war die AIDS-Operation KGB und Stasi: Ab Mitte der 1980er Jahre verbreiteten Agenten Artikel, in denen behauptet wurde, HIV sei eine Biowaffe der USA, und wuschen die Behauptung durch ausländische Zeitungen und Pseudoexperten, bis sie weltweit Widerhall fand. Nach dem Kalten Krieg bestätigten die Beamten die Urheberschaft der Operation; Historiker präzisierten später den Codenamen als Operation Denver (im Volksmund als Operation INFEKTION bekannt). Der Schaden der Kampagne für die öffentliche Gesundheit – der Misstrauen und riskantes Verhalten schürt – bleibt ein warnendes Beispiel für die realen Kosten von Desinformation.

Kommerzielle Ära des Internets und der Suche (1990er bis 2008). Das Web hat das Gatekeeping neu verdrahtet. Suchmaschinen und frühe Foren schufen neue Anreize: Aufmerksamkeit erregen, hoch ranken, über Anzeigen Geld verdienen. "Content Farms" und Low-Friction-Blogs verwischen die Grenzen zwischen Meinung, Gerücht und Berichterstattung. Foren und Ketten-E-Mails sozialisierten "Peer-to-Peer-Glaubwürdigkeit", bei der Vertrautheit oft die Verifizierung ersetzt. Das Muster, das sich hier abzeichnet – für Klicks optimieren und dann eine Erzählung auffüllen – wird sich auf sozialen Plattformen nur noch verstärken.

Plattformaufstieg und algorithmische Feeds (2008–2013). Der News Feed von Facebook, YouTube-Empfehlungen und Twitter-Trendlisten machten die Verbreitung sowohl personalisiert als auch undurchsichtig. Microtargeting-Anzeigen ermöglichen es Akteuren, Botschaften zu geringen Kosten zu testen und zu iterieren. Das Plattform-Governance-Modell – reaktiv, in großem Maßstab – hatte Mühe, mit koordinierten Netzwerken, Sockenpuppen und "Engagement Hacking" Schritt zu halten, das Neues, Empörung und Identität ausnutzt.

Vernetzte Abläufe werden zum Mainstream (2014–2018). Russlands Informationsoperationen rund um die Ukraine und die Wahlen im Westen zeigten eine plattformübergreifende Koordination. Die Internet Research Agency (IRA) betrieb Tausende von Personas, Seiten und Gruppen, um soziale Spaltungen auszunutzen; US-Ermittlungen und der Geheimdienstausschuss des Senats dokumentierten die Reichweite und die Taktiken, während die Plattformen begannen, IRA-Eigentum in großem Umfang zu entfernen. Parallel dazu löste der Abschuss von MH17 über der Ukraine im Jahr 2014 einen rasanten Kreislauf aus konkurrierenden Narrativen, manipulierten Bildern und offizieller Verschleierung aus. Open-Source-Ermittler (insbesondere Bellingcat) konterten mit Geolokalisierung, der Rückverfolgung von Waffensystemen und der Rekonstruktion der Zeitleiste – ein entscheidender Moment für die Rolle von OSINT bei der Entlarvung staatlicher Desinformation.

Verschlüsselte Chats, Randplattformen und die "Infodemie" (2019–2021). Messaging-Apps und alternative Plattformen verringerten die Sichtbarkeit der Moderation und erhöhten die Viralität in geschlossenen Netzwerken. Während der COVID-19-Pandemie bezeichnete die WHO die Krise als Infodemie – eine Überfülle an Informationen (wahr, falsch und alles dazwischen), die zu Verwirrung und gefährlichen Verhaltensweisen führte. In der Pandemie-Ära wurde die "evidenzgeformte Identität" normalisiert, bei der Gemeinschaften maßgeschneiderte Realitäten aus Memes, Videos und manipulierten Screenshots schneller zusammensetzten, als die Institutionen reagieren konnten.

Krieg und Plattformen treffen OSINT in großem Maßstab (2022–2023). Russlands groß angelegter Einmarsch in die Ukraine hat sowohl die Manipulation als auch die Gegenmanipulation beschleunigt. Einflussnetzwerke betrieben geklonte Kanäle und Imitationsseiten – am sichtbarsten die Operation Doppelgänger, die europäische Medien und Ministerien parodierte, um anti-ukrainische Narrative zu verbreiten und die Unterstützung zu untergraben. Ermittler und Regierungen deckten den Technikmix auf: ähnlich aussehende Domains, kopierte Seitenvorlagen, geseedete Geschichten und Anzeigenkäufe, um die Reichweite zu steigern. In der Zwischenzeit fusionierten Open-Source-Communities und professionelle Redaktionen Methoden – Satellitenbilder, Sensordaten, Videos vor Ort –, um Behauptungen nahezu in Echtzeit zu widerlegen und das Informationsgleichgewicht in Richtung einer transparenten Verifizierung zu verschieben.

Ära der generativen KI (2023–2025). Die billige Synthese veränderte die Kostenkurve. Texte, Bilder, Stimmen und Videos können jetzt in großem Maßstab fabriziert oder subtil verändert werden. Schauspieler mit geringem Aufwand können Kampagnen durchführen, bei denen Quantität vor Qualität steht, die sich authentisch genug anfühlen, um ein lockeres Scrollen zu bestehen. Bei den Wahlen in der realen Welt begannen konkrete Schäden zu verzeichnen: Im Januar 2024 versuchten KI-generierte Robocalls, die Präsident Biden nachahmten, die Wahlbeteiligung in New Hampshire zu beeinflussen; Die US-Regulierungsbehörden

reagierten, indem sie KI-Stimmen in automatischen Anrufen verboten und Geldstrafen und Anklagen gegen die beteiligten Organisatoren und Netzbetreiber verhängten. Gleichzeitig begannen Plattformen und Verlage mit der Erprobung von Provenienz-Tools wie C2PA/Content Credentials, die überprüfbare Bearbeitungsverläufe in Mediendateien einbetten. Der Ansatz ist vielversprechend, hängt aber von der Akzeptanz des Ökosystems und der Klarheit der Benutzeroberfläche ab.

Die regulatorische Wende in Europa (2022–2025). Die EU hat freiwillige Maßnahmen durch verbindliche Regeln ergänzt. Der Strengthened Code of Practice on Disinformation (2022) hat die Demonetarisierungs- und Transparenzverpflichtungen von Plattformen, Werbenetzwerken und Faktenprüfern vorangetrieben, während Evaluierungen auf eine ungleiche Einhaltung hinweisen. Mit dem Digital Services Act (DSA) wurden dann rechtliche Verpflichtungen und Durchsetzungsbefugnisse festgelegt, die seit dem 17. Februar 2024 uneingeschränkt auf Plattformen anwendbar sind, darunter systemische Risikobewertungen (z. B. Desinformation), Datenzugang für geprüfte Forscher und erhebliche Geldstrafen bei Verstößen. Forscher und die Zivilgesellschaft untersuchen nun, wie sehr diese Maßnahmen die Monetarisierung und den Zugang zu Desinformation in der Praxis reduzieren, während die Regulierungsbehörden den DSA anhand realer Fälle testen (einschließlich Operationen im Stil von "Doppelgängern").

Was sich tatsächlich geändert hat – und was nicht. Das Medium hat sich von Print zu Broadcast und Feeds zu Basismodellen entwickelt, aber das Playbook dreht sich immer noch um Aufmerksamkeitserfassung, Identitätssignale und narrative Wiederholung. Die Billigkeit der Erstellung und die Undurchsichtigkeit der Kuration (Empfehlungssysteme, private Gruppen, verschlüsselte Kanäle) haben das Feld in Richtung Skalierbarkeit und Geschwindigkeit gekippt. Transparente Verifizierung, offene Archive und Provenienzstandards geben den Verteidigern jedoch einen Hebel – insbesondere in Kombination mit Pre-Bunking- und Community-Messengern. Bemerkenswert ist, dass die messbaren Auswirkungen der Exposition gegenüber Inhalten ausländischer Einflussnahme auf individueller Ebene geringer sein können als befürchtet; Die gesellschaftliche Gefahr ist das Aggregat: eine narrative Sättigung, die gemeinsame Fakten untergräbt und institutionelle Zeit verbraucht.

Mit dem Faktencheck beginnen

Bevor wir mit der Faktenprüfung beginnen, wollen wir verstehen, wie Fehlinformationen funktionieren und warum selbst intelligente Menschen falsche Dinge glauben. Wir werden kurz besprechen, wann und wie man reagiert und welche Ethik es mit der Faktenprüfung zu tun hat.

Nachdem wir die Konzepte abgestimmt haben, springen wir zu den 5/10/30 Workflows während der Live-Arbeit. Konsultieren Sie Tools & Techniken für spezifische Methoden und studieren Sie die europäischen Fallstudien für End-to-End-Beispiele. Halten Sie den Kreislauf am Laufen, indem Sie Erkenntnisse in zukünftige Verbesserungen einfließen lassen. Am Ende stellen wir Länder-Playbooks für die an unserem Projekt teilnehmenden Länder vor, die aufzeigen, wie die zuvor besprochenen Jahre lokalisiert werden können und welche verlässlichen Quellen zu verwenden sind. Basierend auf den Beispielen können Sie für jedes Land ein Playbook erstellen. Zusammenfassend:

1. Beginnen Sie hier, um sich auf Konzepte und Ethik abzustimmen.
2. Wechseln Sie zu Workflows (15/10/30), um Schritt-für-Schritt-Aktionen zu erhalten.
3. Konsultieren Sie Tools & Techniken für spezifische Überprüfungen (Bilder, Zahlen, Zitate, Netzwerke).
4. Studieren Sie europäische Fallstudien, um die Workflows durchgängig zu sehen.
5. Sehen Sie sich das Länder-Playbook an Ihrem spezifischen Standort an

Wie Desinformation funktioniert

Desinformation ist nicht nur ein falscher Beitrag oder ein gefälschtes Bild – sie ist ein **System**. Es verbreitet sich aufgrund der Art und Weise, wie Informationen online erstellt, geteilt und darauf reagiert werden. Das Verständnis, wie dieses System funktioniert, hilft Botschaftern, Muster schnell zu erkennen und die richtige Reaktion zu wählen.

1. Es beginnt mit einem Schauspieler

Jemand erstellt oder verstärkt irreführende Inhalte. Es kann sein:

- Eine Person mit starken Meinungen
- Eine koordinierte Gruppe oder ein koordiniertes Netzwerk
- Ein Bot oder ein automatisiertes Konto
- Ein Medium mit einer Agenda
- Ein staatlicher Akteur, der versucht, die Meinung zu beeinflussen

Die entscheidende Frage: *Wem nützt es, wenn die Menschen das glauben?*

2. Es verwendet strategisches Verhalten

Desinformation verbreitet sich selten zufällig. Zu den gängigen Verhaltensweisen gehören:

- Dieselbe Nachricht auf vielen Konten posten
- Emotionale Sprache verwenden, um Reaktionen zu provozieren
- Automatisieren von Beiträgen, um das Volumen zu erhöhen
- Für Anzeigen bezahlen oder Inhalte bewerben
- Umleiten von Benutzern über verdächtige Links

Diese Verhaltensweisen tragen dazu bei, dass falsche Behauptungen schneller mehr Menschen erreichen.

3. Inhalte sind so gestaltet, dass sie Emotionen auslösen

Desinformation funktioniert am besten, wenn sie den Menschen das Gefühl gibt:

- Empörung
- Furcht
- Stolz
- Bedroht oder unsicher

Starke Emotionen veranlassen Menschen, zu teilen, bevor sie denken. Bilder, kurze Videos und einfache Slogans werden oft verwendet, weil sie kritisches Denken umgehen.

4. Das Ziel ist Aufmerksamkeit, nicht Genauigkeit

Desinformation verbreitet sich, weil Plattformen Folgendes belohnen:

- Interaktionen
- Klicks
- Geteilte Inhalte
- Kommentare

Je emotionaler oder reißerischer der Inhalt ist, desto mehr pusht der Algorithmus ihn. Falsche Inhalte müssen nicht überzeugend sein – sie müssen nur Aufmerksamkeit erregen.

5. Grad: Es verbreitet sich über Netzwerke

Ein einzelner Beitrag kann keinen Schaden anrichten, aber Netzwerke können:

- Wiederholen Sie dieselbe Nachricht von verschiedenen Konten
- Koordinieren Sie das Posten zu bestimmten Zeiten
- Nutzen Sie Influencer, um ihm Glaubwürdigkeit zu verleihen
- Bewegen Sie das gleiche Narrativ auf allen Plattformen (FB → TikTok → Telegram)

Durch diese Wiederholung fühlt sich die Botschaft vertraut und daher "wahr" an.

6. Wirkung: Es zielt darauf ab, Überzeugungen oder Verhaltensweisen zu beeinflussen

Desinformation versucht:

- Vertrauen in Institutionen beschädigen
- Polarisation erhöhen
- Entmutigung zur Wahl oder Teilnahme
- Verbreiten Sie Angst oder Unsicherheit
- Manipulation der öffentlichen Meinung oder des öffentlichen Verhaltens

Die Auswirkungen können für jede Person gering sein, aber auf Gemeindeebene groß.

7. Warum die Leute daran glauben

Menschen sind verwundbar, wenn Inhalte:

- Bestätigt ihre bestehenden Überzeugungen
- Passt zu ihrer Weltanschauung
- Scheint von jemandem "wie ihnen" zu kommen
- Zeigt eine dramatische Geschichte oder ein schockierendes Bild

Das ist normale menschliche Psychologie – kein Fehler.

8. Die gute Nachricht: Einfache Checks funktionieren

Die meisten Desinformationen können frühzeitig gestoppt werden durch:

- Überprüfen der Quelle
- Suche nach dem Originalbild oder -video
- Suche nach früheren Versionen der Behauptung
- Pausieren vor dem Teilen
- Frage: *Was ist die Absicht hinter diesem Beitrag?*

Desinformation beruht auf Geschwindigkeit. Faktenprüfer setzen auf Klarheit. Wenn Sie auch nur für 10 Sekunden langsamer werden, wird der Kreislauf unterbrochen.

Die ABCDE-Linse ist eine *praktische Möglichkeit, das System hinter einer einzigen Behauptung zu sehen. ABCDE verlagert Sie von Post-by-Post-Reaktionen auf das Systembewusstsein: Akteur, Verhalten, Inhalt, Grad und Wirkung. Führen Sie es aus, bevor Sie Ressourcen binden, damit die Sichtung und die Strategie aufeinander abgestimmt sind. Fixieren Sie sich nicht nur auf Inhalte – Signale über Akteure und potenzielle Auswirkungen bestimmen oft die*

proportionalen Reaktionen. Jede Anwendung sollte mit einer kurzen Empfehlung enden, was als nächstes zu tun ist.

A – Akteur: Wer erstellt/verstärkt den Inhalt? Individuelles, koordiniertes Netzwerk, Bot, Medium, NGO, staatlicher Akteur? Wie sieht ihre Erfolgsbilanz und ihre erklärten Interessen aus?

B – Verhalten: Posting-Kadenz, plattformübergreifende Koordination, Astroturfing, Brigading, Bot-ähnliche Signale, Monetarisierungsmuster.

C – Inhalt: Was wird behauptet? Genaue Formulierungen, verwendete Daten, Bearbeitungen, Bilder, emotionale Auslöser, fehlender Kontext.

D – Ausmaß: Wie weit verbreitet und wirkungsvoll? Ist es eine Nische, ein Trend oder Mainstream? Welche Zielgruppen werden angesprochen?

E – Wirkung: Welcher Schaden könnte daraus resultieren (Sicherheit, öffentliche Gesundheit, bürgerliches Vertrauen)? Welche Gegenmaßnahmen sind verhältnismäßig?

Verwenden Sie ABCDE, um zu entscheiden, ob, wie stark und wo eingegriffen werden soll (öffentlicher Beitrag, private Nachricht, organisatorische Erklärung, Medienanfrage).

Menschliche Psychologie: Warum kluge Menschen falsche Dinge glauben

Falsche Informationen zu glauben bedeutet nicht, dass jemand ungebildet oder nicht intelligent ist. Tatsächlich können kluge Menschen genauso verwundbar sein – manchmal sogar noch verwundbarer. Dies geschieht, weil Desinformation mit der menschlichen Psychologie zusammenarbeitet, nicht gegen sie. Vorurteile, Identität und Emotionen prägen, wie Menschen Korrekturen erhalten. Überprüfen Sie Ihre Botschaften auf gängige Fallstricke und klassische Propagandainstrumente, damit sie nicht nach hinten losgehen. Vermeiden Sie es, die falsche Behauptung in den Schlagzeilen zu beschämen und zu wiederholen. Streben Sie nach wahrheitsorientierten, respektvollen Erklärungen, die zum Dialog einladen.

- Kognitive Verzerrungen:
    - Bestätigungsfehler (wir suchen nach Beweisen, mit denen wir bereits einverstanden sind)
    - Verfügbarkeitsverzerrung (aktuelle oder lebhafte Geschichten fühlen sich wahrscheinlicher an)
    - Motiviertes Denken (wir verteidigen unsere Identität, nicht die Fakten)
- Propagandamittel (klassisches Drehbuch): Beschimpfungen, glitzernde Allgemeinheiten, Transfer, Zeugnisse, einfache Leute, Kartenstapeln (gezieltes Weglassen widersprechender Informationen), Bandwagon.

- Emotionale Dynamik: Angst, Empörung und Identitätsstolz erhöhen die Teilbarkeit und verringern die Kontrolle.

Praktische Implikation: Botschafter sollten Verifizierung mit einfühlsamer Kommunikation verbinden – mit Klarheit und nicht mit Verachtung führen. Konzentrieren Sie sich darauf, die verifizierte Wahrheit zu teilen, und beweisen Sie nicht, dass andere falsch liegen. Vermeiden Sie Beschämung – sie schließt das Gespräch. Verwenden Sie klare, einfache Erklärungen. Sprechen Sie Emotionen an, nicht nur Fakten.

Wenn Sie diese psychologischen Punkte verstehen, können Sie so kommunizieren, dass die Menschen tatsächlich hören können. Die Wahrheit verbreitet sich am besten, wenn sie sich respektvoll, menschlich und zuordenbar anfühlt.

Entscheiden, wann und wie reagiert wird

Passen Sie die Reaktionsintensität an das reale Risiko und die Reichweite an, um zu vermeiden, dass kleinere Inhalte verstärkt werden. Kombinieren Sie "Grad" und "Wirkung", um zwischen privater Klarstellung, einem kurzen öffentlichen Beitrag, einer vollständigen Erklärung oder einer Koalitionsbotschaft zu wählen. Seien Sie vorsichtig, wenn Sie Zitate twittern oder die Unwahrheit prominent wiederholen. Legen Sie einen Überwachungsplan fest, der festlegt, wer was, wo und wie oft überprüft.

- Greifen Sie ein, wenn das Narrativ an Zugkraft gewinnt, Schäden plausibel sind, Ihre NGO benannt wird oder Ihre Gemeinschaft ins Visier genommen wird.
- Reaktion auf Risiko anpassen:
    - Geringes Risiko, geringe Reichweite: Stille Aufklärung des Einzelnen.
    - Mittleres Risiko: kurzer öffentlicher Beitrag mit einer klaren Korrektur und einem maßgeblichen Link.
    - Hohes Risiko / koordiniert: vollständige Erklärung, Koalitionsbotschaften, Medienengagement und proaktives Prebunking.
- Vermeiden Sie Sauerstofffallen: Wiederholen Sie die falsche Behauptung nicht in Schlagzeilen; Führe mit der Wahrheit und sprich dann die Lüge an.

Ethik & Sorgfaltspflicht

Leitplanken schützen Würde, Sicherheit und Vertrauen, während Sie verifizieren und kommunizieren. Fragen Sie sich vor der Veröffentlichung, ob Sie den Schaden minimieren, Unsicherheiten transparent machen, Freiwillige schützen und gesetzliche und Markenregeln einhalten. Vermeiden Sie Doxxing, unnötige persönliche Daten und DSGVO-Probleme;

Protokollieren Sie Belästigungen und eskalieren Sie Bedrohungen. Verwenden Sie eine Ethik-Checkliste, ein Sicherheitsprotokoll und einen kurzen Compliance-Hinweis.

- Respekt & Würde: Kritik behauptet, nicht Menschen.
- Verhältnismäßigkeit: Unbeabsichtigte Verstärkung in Betracht ziehen; Wählen Sie die Kanäle entsprechend aus.
- Transparenz: Teilen Sie Methoden, Quellen und Unsicherheiten.
- Sicherheit: Schützen Sie bei Bedarf die Identität der Freiwilligen; Belästigung im Protokoll; Eskalieren Sie Bedrohungen.
- Compliance: Befolgen Sie die Marken-, Rechts- und Datenschutzregeln Ihrer Organisation.

Arbeitsabläufe

Die 5/10/30-Minuten-Workflows sind unsere zeitlich begrenzten Drehbücher, um Faktenchecks unter realem Druck gut durchzuführen: eine 5-minütige SIFT-Triage, um versehentliche Verstärkungen zu vermeiden, eine 10-minütige prägnante Prüfung, die ein kurzes, verknüpfbares Urteil mit einem Vertrauensetikett liefert, und eine 30-minütige vollständige Prüfung, die Beweise, Kontext (ABCDE), Ethik und eine verhältnismäßige Antwort dokumentiert. Wir beziehen sie ein, um gute Absichten in wiederholbare Maßnahmen umzusetzen – damit jeder Botschafter, unabhängig von seiner Erfahrung, die gleichen Schritte befolgen, eine gleichbleibende Qualität erreichen, einen transparenten Prüfpfad hinterlassen und die am wenigsten verstärkende Antwort wählen kann, die das Vertrauen unserer Community dennoch schützt.

Am Ende dieses Abschnitts stellen wir auch kurze Tutorials zur Verfügung, die effektiv in Echtzeit genutzt werden können, um auf Desinformation zu reagieren, und die im Lernprozess nützlich sein können.

Hier sind die wesentlichen 5/10/30-Minuten-Workflows für Ihr Toolkit.

5 Minuten – SIFT Quick Triage (vor dem Teilen/Weiterleiten)

Ziel: Entscheiden Sie sich für "Ignorieren / Für später speichern / schnell klären", ohne in Fallen zu tappen.

1) **Stopp**. Atmen. Nicht verstärken. Erfassen Sie den Beitrag/Link/Screenshot (URL + Zeitstempel). Wenn es sich um eine Story/Reel handelt, nehmen Sie den Bildschirm auf und notieren Sie sich die Zeit.

2) **Untersuchen Sie die Quelle**. Wer hat es veröffentlicht? Was ist ihre Erfolgsbilanz/Expertise? Wie werden sie finanziert? Wer hat es weiter geteilt und warum? Wenn es behauptet, ein bekanntes Medium oder ein Journalist zu sein, überprüfen Sie die offizielle Kontaktseite und vergleichen Sie Domains (Spot Typosquats/Clones/Impersonation).

3) **Finden Sie eine bessere Abdeckung.** Öffnen Sie zwei unabhängige Registerkarten (seitliches Ablesen). Durchsuchen Sie die Kernanspruchsformulierung + site:-Operatoren. Suchen Sie nach primären oder maßgeblichen Quellen (offizielle Statistiken, Gerichts-/Behördenerklärungen, seriöse Medien).

4) **Rückverfolgung zum Ursprung.** Scrollen Sie zur frühesten Version, die Sie finden können. Wenn visuell: Führen Sie Google Lens/TinEye schnell aus – sehen Sie frühere Daten oder andere Kontexte?

5) **Entscheiden + Risiko beachten**. Wenn es nach einem Kampagnenelement riecht (Bots, identische Copy-Bursts, Influencer-Hottakes, "zu ausgefeilte" Klonseiten), beteiligen Sie sich noch nicht öffentlich. Notiz: Art der Behauptung (Ereignis/Zahl/Zitat/Bild/Video), Vertrauen

(gering/unbekannt) und ob dies bekannte gesellschaftliche Schwachstellen treffen könnte (Polarisierung, geringe Medienkompetenz, geringes Vertrauen usw.).

Ausgaben (≤60 Wörter): Ein-Absatz-Triage-Notiz mit Links, frühestem Erscheinen, schnellem Quellenurteil und nächster Aktion (Ignorieren / Privat fragen / 10-Minuten-Prüfung).

10 Minuten — Concise Verification (veröffentlichungsfähiges Micro-Finding)

Ziel: Erstellen Sie ein kurzes, verknüpfbares Ergebnis mit einem Konfidenzlabel.

0) Einrichtung. Erstellen Sie ein Mini-Protokoll: Anspruch, URL(s), Screenshot(s), Zeitstempel(n). Archivieren Sie wichtige Links (Wayback oder Perma.cc). Klassifizieren: mis / dis / mal / ungeprüft.

1) Klassifizieren Sie die Art der Reklamation und wählen Sie die richtigen Mikrotools aus. Bild: Speichern Sie die Datei → Google Lens/TinEye → vergleichen Sie die früheste Verwendung und höher aufgelöste Übereinstimmungen → suchen Sie nach Zuschnitten/Bearbeitungen.

- Video: Extrahieren Sie 3 bis 5 Keyframes (Rechtsklick-Frame oder ein Keyframe-Werkzeug) → kehren Sie Frames um (Reverse Image Search). Der Scan nach KI-Indikatoren zeigt: Lippensynchronisation/A-V-Diskrepanz, glasiger Blick, zu glatte Haut, deformierte Hände, übermäßig saubere/monotone Stimme.
- Zitat/"X sagte Y": Suchen Sie nach der genauen Phrase in Anführungszeichen + Website: von offiziellen Seiten oder seriösen Verkaufsstellen.
- Zahl/Statistik: Identifizieren Sie den primären Datensatz; Überprüfen Sie die neueste offizielle Veröffentlichung (Methode, Zeitspanne, Vorbehalte).
- Konto/Quelle: Überprüfen Sie das Alter / den Registrar der Domain, das TLS-Zertifikat, die Info-/Kontaktseite, die Verfasserzeilen. Vergleichen Sie mit der Website des legitimen Outlets (erkennen Sie geklonte Layouts/Typosquats). Werfen Sie einen Blick in die Posting-Historie für Copy-Paste-Bursts und koordinierte Hashtags (Verhaltenssignal).

2) Kreuzvalidierung. Öffnen Sie mindestens zwei unabhängige Bestätigungen (Behörde + seriöse Berichterstattung). Wenn keine: Sagen Sie nicht verifiziert und was würde es bestätigen.

3) Grad & Wirkung (schnell). Breitet es sich über eine Nische hinaus aus? Wer ist betroffen? Gibt es sichtbare Geoblocking-/Weiterleitungsketten/Anzeigen? Achten Sie darauf, ob es bekannte Schwachstellen in der Community ausnutzt.

4) Mikro-Aufzeichnung. Zwei Sätze: was behauptet wird; was Sie gefunden haben (mit stärkstem Link). Ein Satz: Zuversicht + Vernunft ("frühester Fall aus dem Jahr 2019 zeigt einen anderen Kontext"; "Kein Datensatz im primären Datensatz"). Ethik-Check: Vermeiden Sie es, die

Unwahrheit in der Überschrift zu verstärken; Geben Sie keine unnötigen personenbezogenen Daten an.

Ausgaben:

- 1-Absatz-Urteil (Wahr / Falsch / Irreführend / Nicht verifiziert) mit Zuversicht.
- 3 Links (Herkunft, beste alternative Berichterstattung, primär/offiziell).
- Label-Antwort: stille Klarstellung / kurzer öffentlicher Beitrag / Eskalation auf 30-Minuten-Prüfung.

Häufige Fallstricke, die es zu vermeiden gilt: emotional aufgeladenes Framing, Statistiken ohne Quellen, "professionell aussehende", aber maskierte Websites und identitätsstiftende Propagandainstrumente.

30 Minuten — Vollständige Überprüfung (reproduzierbar, für die Öffentlichkeit bereit)

Ziel: Ein transparenter, archivierter Erklärer mit einer Anleitung zur proportionalen Reaktion.

0) Admin & Sicherheit. Starten Sie eine Notiz (Datum, Team, überwachte Kanäle). Archivieren Sie alle Schlüssel-URLs (Wayback/Perma). Wenn Belästigungs- oder Doxxing-Risiko besteht, wechseln Sie zu sichereren Kommunikationssystemen. Vorfälle zu protokollieren (Sorgfaltspflicht).

1) Karte ABCDE. Schauspieler: Wer entsteht und wer verstärkt? Gibt es Anzeichen für staatsnahe Medien, Persona-Farmen, bezahlte Trolle, Botnets, Influencer? Verifizieren Sie legitime Journalisten/Medien über offizielle Seiten (keine Nachahmung).

- Verhalten: Typosquattierte/geklonte Domains, kopierte Vorlagen, Redirect-Ketten, bezahlte Anzeigen, Geoblocking, synchronisiertes Posting, Kommentarbrigaden, manipuliertes Chatbot-"Flooding". Dokument mit Screenshots + Zeitstempeln.
- Inhalt: Genaue Formulierungen, Bilder, Bearbeitungen/Ausschnitte, emotionale Hinweise, fehlender Kontext. Vergleichen Sie mit den frühesten Erscheinungen aus Lens/TinEye oder Keyframe-Suchen.
- Grad: Reichweite/Geschwindigkeit/Zielgruppen; Suchen Sie nach Monetarisierungsaufhängern; Beachten Sie die beteiligten Plattformen.
- Wirkung: Wahrscheinliche Schäden (öffentliche Sicherheit, bürgerliches Vertrauen, Reputation). Wählen Sie den effektivsten Kanal mit der geringsten Verstärkung für die Antwort.

2) Stapel von Beweisen

- Primär/offiziell: Datensätze, Rechts-/Behördendokumente, aktenkundige Erklärungen.

- Unabhängige Berichterstattung/Experten: seriöse Medien, anerkannte Spezialisten.
- Technische Checks: WHOIS/Domain-Alter, TLS-Zertifikate; C2PA/Content Credentials (falls vorhanden); EXIF/Metadaten (falls verfügbar); Stil/Zeit/Wetter/Orientierungspunkt prüft die Geolokalisierung (Street View/Mapillary, Sonne/Schatten).
- Kampagnenelemente: Feindseliges Goal Framing, Trolle/Bots, Algorithmus-Gaming, Influencer und Journal-/Wissenschaftsmaskerade – Beispiele für Capture.

3) Verletzlichkeitslinse. Beachten Sie den Kontext: Polarisierung, geringe Medienkompetenz, Ungleichheit, schwache Cybersicherheit, geringes Vertrauen, schwache Regulierung. Wenn Sie mehrere "Ja" haben, priorisieren Sie Prebunk + Tipps zur Medienkompetenz in der Antwort.

4) Analyse & Schlussfolgerung. Schreiben Sie eine kurze Erklärung mit:

- Eine Überschrift, die mit der Wahrheit führt (nicht mit der Lüge).
- 3-Punkte-Zusammenfassung (was wahr/falsch ist, was fehlt, warum es wichtig ist).
- Methode (was Sie überprüft haben, wie).
- Urteil + Vertrauen (Wahr / Falsch / Irreführend / Nicht verifiziert + Hoch / Mittel / Niedrig).
- Quellen & Archive (Herkunft, stärkste Evidenz, Alternativen).
- Verhältnismäßige Reaktion (stille Öffentlichkeitsarbeit / kurze öffentliche Korrektur mit 1 maßgeblichen Link / vollständiger Beitrag + Koalitionskoordination / Medienanfrage).
- Sicherheits- und Ethikhinweis (Privatsphäre respektiert, Unsicherheit angegeben, kein Doxxing).

5) Veröffentlichen & Überwachen. Wählen Sie Kanäle aus, die die Verstärkung minimieren, aber das betroffene Publikum erreichen. Fügen Sie einen Überwachungsplan hinzu: Wer beobachtet welche Plattformen 48–72 Stunden lang? Wann aktualisieren/zurückziehen.

Öffentliche Erklärungsvorlage

- Titel: Führen Sie mit verifizierter Wahrheit (vermeiden Sie die Wiederholung der falschen Behauptung).
- Zusammenfassung (3 Aufzählungspunkte): [A], [B], [C].
- Was wir überprüft haben: [Behauptung, wo sie auftauchte, früheste Instanz].
- Wie wir überprüft haben: [Tools: Lens/TinEye/keyframes/WHOIS/dataset X].
- Was wir gefunden haben: [Prägnante Erzählung mit Links].

- Urteil und Vertrauen: [z. B. Irreführend – mittleres Vertrauen].
- Warum es wichtig ist: [Auswirkung auf die Gemeinschaft/Entscheidung].
- Quellen & Archive: [URLs + Archivlinks].
- Hinweise zu Einschränkungen und nächsten Schritten: [Was würde das Vertrauen stärken].
- Kontakt: [Adresse der Kommunikation von NGO/AF].

Werkzeuge und Techniken

Diese Werkzeuge und Techniken sind das praktische "Wie" unseres Toolkits – die wiederholbaren Methoden, die Skepsis in eine zuverlässige Verifizierung verwandeln. Sie decken den gesamten Bogen einer Behauptung ab: Provenienz und Quellentriage; Bild-, Video- und Audiochecks (inkl. KI-Manipulationshinweise); Angebots- und Datenüberprüfung; Domain-/Website-Forensik für Typosquats und Klone; Triage sozialer Netzwerke; OSINT Geo-/Chrono-Standort; Erkennung von Kampagnenmustern mit ABCDE; die Verwundbarkeitslinse, um maßgeschneiderte Reaktionen zu finden; sowie Ethik, Sicherheit und Archivierung für die Rückverfolgbarkeit. Wir stellen sie zur Verfügung, damit jeder Botschafter schnell und konsequent handeln kann, versehentliche Amplifikationen vermeiden, transparente, reproduzierbare Ergebnisse liefert und die am wenigsten verstärkende Reaktion wählt, die das Vertrauen unserer Gemeinschaft dennoch schützt.

Provenienz und Quellentriage

Verwendung: Erster Kontakt mit einer Reklamation.

Wie: Überprüfen Sie den Verlag, die Erfolgsbilanz, den Anspruch auf Expertise, die Finanzierung und wer sie erweitert hat. Öffnen Sie unabhängige Tabs (laterales Lesen) und vergleichen Sie die Domain mit der offiziellen Website des Outlets, um Imitationen und Typosquats zu erkennen.

Ausgaben: Einzeiliges Quellenurteil + Link(s) zur offiziellen Kontakt-/About-Seite.

Fallstricke: Glaubwürdigkeit durch Design (professionell aussehend, aber gefälscht), Appell an Autorität ohne überprüfbare Referenzen.

Visuelle Verifizierung (Bilder)

Verwendung: Fotos, Screenshots, Memes, "Beweisbilder".

Wie: Speichern Sie die Datei → führen Sie Google Lens und TinEye aus, → früheste Darstellungen und Übereinstimmungen mit höherer Auflösung zu finden → nach Zuschnitten/Bearbeitungen oder wiederverwendeten Bildern in neuen Kontexten zu suchen.

Ausgaben: URL für die früheste Übereinstimmung + Datum, 1–2 Vergleichslinks, Urteil (ursprünglich/bearbeitet/wiederverwendet).

Fallstricke: Sich auf eine einzige Engine verlassen; Sprach-/Regionsfilter ignorieren; Vergessen der Archivierung.

Video- und Audioverifizierung (einschließlich KI-Hinweise)

Verwendung: Clips, Reels, Reden, Sprachnotizen.

Wie: Extrahieren Sie 3 bis 5 Keyframes → suchen Sie sie zurück, vergleichen Sie Audio und Mundbewegungen, achten Sie auf zu saubere, monotone Klangfarben. Verwenden Sie die Liste der KI-Video-Tells: Lippen-Sprach-Diskrepanz, A/V-Desynchronisation, glasiger Blick/kein Blinzeln, zu glatte Haut, deformierte Hände/Finger, Roboterlieferung.

Ausgänge: Keyframe-Matches, kurze A/V-Konsistenznotiz, Urteil + Vertrauen.

Fallstricke: Urteilen nach "Stimmung"; Ignorieren von Unstimmigkeiten zwischen Raumakustik und Beleuchtung; Vergessen, dass echtes Video von geringer Qualität "KI-isch" aussehen kann.

Überprüfung von Angeboten/Ansprüchen

Wann zu verwenden: "X sagte Y", virale Screenshots von Posts, Überschriften.

Wie: Suchen Sie nach der genauen Phrase in Anführungszeichen, überprüfen Sie offizielle Kanäle (Presseseiten, verifizierte Konten), vergleichen Sie Zeitstempel. Suchen Sie nach Screenshots, suchen Sie nach dem Originalbeitrag oder der archivierten Kopie, bevor Sie einem zugeschnittenen Bild vertrauen.

Ausgaben: Link zur ursprünglichen oder maßgeblichen Ablehnung/Bestätigung; Urteil + Vertrauen.

Fallstricke: Gefälschte Screenshots; Satire aus dem Zusammenhang gerissen; Zitatfragmente, die die Bedeutung verdrehen.

Daten, Zahlen & Grafiken

Verwendung: Umfragen, Kriminalitätsstatistiken, Gesundheitszahlen, "Studie zeigt".

Wie: Identifizieren Sie den primären Datensatz, überprüfen Sie das Zeitfenster, die Methode, den Nenner und die Ausschlüsse und berechnen Sie nach Möglichkeit eine einfache Überprüfung neu. Beachten Sie die Unsicherheit und die Fehlerspanne.

Ausgaben: Link zur Primärquelle, Ein-Satz-Methodenhinweis, korrigierte Abbildung (falls erforderlich).

Fallstricke: Herausgepickte Bereiche, Prozent- vs. Prozentpunkte, Modellprojektionen, die als Beobachtungen behandelt werden.

Website- und Domain-Forensik

Verwendungszeit: Verdacht auf geklonte Outlets, Typosquats, Redirect Chains.

Wie: Vergleichen Sie die Rechtschreibung von Domains und TLD mit dem echten Outlet; überprüfen Sie WHOIS/Erstellungsdatum, TLS-Zertifikat, Bylines und Abschnitts-Slugs; folgen Sie Links, um zu sehen, ob sie über Weiterleitungen oder geoblockierte Routen führen. Protokollieren Sie Anzeigen, die nur auf dem Klon erscheinen (Verhaltenssignal).

Ausgaben: Side-by-Side-Domain-Fakten (Alter/Aussteller/Pfade), Screenshots von Layout/Bylines, Urteil (legitim/Klon).

Fallstricke: Die Annahme, dass HTTPS Authentizität impliziert; fehlende subtile Domain-Swaps (rn vs. m).

Triage in sozialen Netzwerken

Verwendung: Konten, Threads, Trendbeiträge.

Wie: Archivieren Sie den Beitrag; scannen Sie den Kontoverlauf nach Copy-Paste-Bursts, Zeitzonenmustern, plötzlichen Follower-Spitzen oder identischen Kommentarzeichenfolgen (Bots/Brigaden). Überprüfen Sie die Hashtag-Choreografie und das Cross-Posting auf anderen Plattformen.

Ausgaben: 3–5 Screenshots mit Zeitstempeln; Hinweis zu Koordinationssignalen; schnelle Gradschätzung (Reichweite/Geschwindigkeit).

Fallstricke: Übermäßige Zuschreibung von Koordination an Fandoms; Ignorieren von Sprachvarianten.

OSINT Geolokalisierung & Chronolokalisierung

Verwendung: "Das ist hier/jetzt passiert"-Behauptungen.

Wie: Zuordnen von Sehenswürdigkeiten über Google Maps/Street View/Mapillary/OpenStreetMap; Vergleichen von Skylines, Straßenmöbeln, Ladenschildern. Schätzen Sie die Zeit mit Sonnen-/Schattenrichtung, Wetterarchiven oder Veranstaltungskalendern.

Ausgaben: Übereinstimmende Koordinaten + Proof-Bilder; Zeitschätzung (falls machbar).

Fallstricke: Renovierungen/neue Beschilderung seit der Bildererfassung; gespiegelte/zugeschnittene Visualisierungen.

Erkennung von Kampagnenmustern (ABCDE-verknüpft)

Verwendung: Wiederkehrende Erzählungen oder Multi-Asset-Pushes.

Wie: Log Actor (staatlich ausgerichtete Medien, Persona-Farmen, Influencer), Verhalten (Imitations-E-Mails, Typosquats, geklonte Layouts, Anzeigen, Weiterleitungsketten, Geoblocking), Content (identische Gesprächspunkte), Grad (plattformübergreifende Verbreitung), Wirkung (Zielgruppe, plausibler Schaden).

Ausgaben: Einseitiges Musterblatt + proportionale Antwortempfehlung.

Fallstricke: Einen Beitrag als Problem behandeln, wenn die Infrastruktur der Punkt ist.

Vulnerability Lens (kontextbezogenes Risiko)

Verwendung: Vor der Veröffentlichung oder Interaktion mit Communities.

Wie: Checkliste ausführen: Polarisierung, Medienkompetenz, sozioökonomische Ungleichheit, schwache Cybersicherheit, geringes institutionelles Vertrauen, schwache Regulierung. Wenn mehrere "Ja", bevorzugen Sie Vorsicht, vorsichtigen Ton und lokale Boten.

Ausgaben: 2-zeilige Kontextnotiz, die die Antwortwahl rechtfertigt.

Fallstricke: Dem Publikum die Schuld geben; die Wissensträger der Gemeinschaft ignorieren.

Ethik, Sicherheit und Compliance

Verwendung: Jede Prüfung vor der Veröffentlichung.

Wie: Wenden Sie die Ethik-Checkliste an: Minimieren Sie den Schaden, vermeiden Sie unnötige personenbezogene Daten, zeigen Sie Unsicherheiten, nutzen Sie den am wenigsten verstärkenden Kanal, protokollieren Sie Belästigungen und eskalieren Sie bei Bedarf, respektieren Sie das Urheberrecht/Einwilligung/DSGVO.

Ausgaben: Kontrollkästchen-Eintrag in der Fallakte.

Fallstricke: Wiederholen der Unwahrheit in Überschriften; Doxxing aus Versehen (Screenshots mit PII).

Archivierung & Rückverfolgbarkeit

Verwendung: Ab dem ersten Klick.

Wie: Speichern Sie Original-URLs, Screenshots mit Zeitstempeln und Archivkopien (Wayback/Perma). Benennen Sie Dateien konsistent. Führen Sie ein kurzes Methodenprotokoll, damit ein Kollege Ihr Ergebnis reproduzieren kann.

Ausgaben: Kompakter Fallordner (Herkunft → Methode → Urteil).

Fallstricke: Verschiebende Ziele (gelöschte Beiträge); fehlende Zeitzonen.

Co-funded by the European Union

Europäische Fallstudien

Bei diesen europäischen Fallstudien handelt es sich um konkrete, reale Szenarien – wie die geklonten Kanäle der Operation Doppelgänger, die OSINT-Rekonstruktion von MH17, das Deepfake-Audio in der Slowakei vor den Wahlen, das Selenskyj-Deepfake "Kapitulation" und Litauens hybride Bot-und-Scam-Pushes –, die es den Botschaftern ermöglichen, die genauen Fähigkeiten in unserem Toolkit unter glaubwürdigen Bedingungen zu üben. Jedes verbindet die Erzählung mit den genauen Signalen, Tools und Arbeitsabläufen, die Sie unterrichten (SIFT • 10-Minuten-Check • 30-Minuten-ABCDE) und stützt sich auf die Praxis im Debunk-Stil. Wir binden sie ein, um abstrakte Methoden in ein Muskelgedächtnis umzuwandeln: Erkennen von Verhaltenssignalen (geklonte Domänen, Weiterleitungen, Bots), Ausführen schneller visueller/akustischer Überprüfungen (Lens, TinEye, Keyframes, KI-Tells), Mapping von ABCDE, um eine proportionale Reaktion auszuwählen, und Dokumentation der Ergebnisse mit Archiven und Konfidenzetiketten. Durch das Üben mit europäischen Beispielen, die unserem Kontext nahe kommen, lernen die Teams, schnell zu handeln, versehentliche Verstärkungen zu vermeiden und das Vertrauen der Gemeinschaft durch transparente, reproduzierbare Verifizierung zu schützen.

"Operation Doppelgänger" – geklonte Verkaufsstellen und Typosquats zielen auf die EU ab

Erzählung. Eine langjährige Beeinflussungsoperation veröffentlicht Artikel über Look-Alike-Domains, die europäische Medien und Institutionen nachahmen, und bewirbt sie dann über Anzeigen, Weiterleitungen und Influencer-Pickup.

Signale & Werkzeuge. Domain-Forensik (Tippfehler/TLD-Swaps, WHOIS-Alter, TLS-Aussteller), Layout-/Byline-/Kontaktseiten-Diskrepanzen; Anzeigen-/Weiterleitungsketten; Geoblocking; Archivierung.

Workflow-Zuordnung. SIFT (Spot-Imitation); 10 Min. (Domain/TLS + früheste Bilderscheinungen über Lens/TinEye); 30 Min. ABCDE (Akteur = Infrastruktur + Verstärkung; Verhalten = Klone/Anzeigen/Weiterleitungen; Grad = plattformübergreifende Streuung; Effekt = Reputations-/Bürgerschaden).

Was ich lehren soll. "Provenance first" schlägt Hot Takes; behandeln Sie die Infrastruktur (Klon-Netzwerk) als die Geschichte, nicht nur als einen Beitrag.

Lesen Sie mehr. EU-DisinfoLab-Übersichten und PDFs; Die Routing-Analyse der Weiterleitungskette von CORRECTIV.

Co-funded by the European Union

MH17 (2014) — OSINT-Geolokalisierung und Rekonstruktion der Zeitleiste

Erzählung. Konkurrierende Behauptungen folgten auf den Abschuss von Flug MH17 über der Ostukraine. Open-Source-Ermittler verfolgten die Route eines Buk-Werfers und verknüpften Bilder, Serienmarkierungen, Straßenschilder und Zeitstempel.

Signale & Werkzeuge. Rückseiten-/Videoprüfungen, Street View/Mapillary, Abgleich von Beschilderungen/Sehenswürdigkeiten, Schatten-/Zeitprüfungen, Archivaufnahmen; strukturiertes Fallnotizbuch.

Workflow-Zuordnung. 10 min (Keyframes → Rückwärtssuche; triangulieren früheste Beiträge); 30 min ABCDE + Evidence Stack (primäre/offizielle Befunde, seriöse Berichterstattung, OSINT).

Was ich lehren soll. Wie reproduzierbare Methoden und Archivierung Vertrauen auf Gerichtsniveau schaffen.

Lesen Sie mehr. Bericht(e) von Bellingcat; spätere Erwähnungen in europäischen Verfahren und Medien.

Slowakei 2023 – Deepfake-Audio-Drop vor den Wahlen

Erzählung. Tage vor der Abstimmung (während der Medienstille) tauchten KI-generierte Audioaufnahmen auf, die sich als Gespräch über Wahlmanipulationen ausgaben, und verbreiteten sich schnell auf sozialen Plattformen und Messaging-Apps.

Signale & Werkzeuge. Grundlagen der Audioforensik (Raumklang, Schnitte, Prosodie); Quellen-/Provenienzlücken; plötzliche plattformübergreifende Aufnahme; Influencer-Verstärkung ohne Primärquelle; blinde Flecken der Plattformpolitik für Audio.

Workflow-Zuordnung. SIFT (nicht verstärken; Originale erfassen; das Risiko der Stille beachten); 10 Minuten (Suche nach exakten Phrasen; Original-Upload suchen; Vergleich mit verifizierten Sprachproben; Log-Unsicherheit); 30 Minuten (Grad und Wirkung → proportionale Reaktion; Anleitung für Partner vor der Veröffentlichung).

Was ich lehren soll. Warum Audio-Deepfakes schwieriger zu kontrollieren sind als Videos – und wie man Unsicherheit klar und schnell kommuniziert.

Lesen Sie mehr. Verdrahtete Erklärung; Bloomberg-Berichterstattung; Vorfalldatenbanken, in denen der Drop und der Zeitpunkt zusammengefasst sind.

Selenskyjs "Kapitulation" Deepfake (2022) – schnelle Entlarvung in Kriegszeiten

Erzählung. Ein gefälschtes Video, in dem Präsident Selenskyj zur Kapitulation auffordert, wurde kurzzeitig online ausgestrahlt (und Berichten zufolge über kompromittierte Kanäle), wurde aber schnell mit einer authentischen Erklärung und der Entfernung von Plattformen gekontert.

Signale & Werkzeuge. KI-Video erzählt: Lippen-/A-V-Ungleichgewicht, glasiger Blick, zu glatte Haut; Keyframe-Rückwärtssuche; Provenienzprüfungen; Überprüfung durch offizielle Kanäle.

Workflow-Zuordnung. 10 Minuten (Keyframes → Rückwärtssuche; Hinweis zur A/V-Konsistenz; Überprüfung auf offiziellem Kanal); 30 min (klare Erklärung, die mit der Wahrheit führt; Archivlinks; Vertrauensetikett).

Was ich lehren soll. Bereitschaft + schnelle, wahrheitsgetreue Botschaften können die Auswirkungen abschwächen, selbst wenn ein Deepfake landet.

Lesen Sie mehr. France24 entlarvt; Euronews-Kontext; Analyse des Playbooks für schnelle Gegenbotschaften.

Litauen (2023–2024) – groß angelegter hybrider Betrug + Desinformationsschub

Erzählung. Debunk.org dokumentierten einen koordinierten Angriff, bei dem betrügerische Seiten, nicht authentische Konten und kremlfreundliche Narrative gemischt wurden, die sich an das litauische Publikum richteten. Spätere Berichte verfolgen Bot-Netzwerke und thematische Pushes (z. B. Kaliningrad-bezogene Inhalte).

Signale & Werkzeuge. Netzwerksignale (Copy-Paste-Bursts, Zeitzonenmuster), Bot-ähnliche Aktivitäten, Kampagnen-Branding, Cross-Posting; Provenienz + Archivierung; Vulnerabilitätsperspektive (geringes Vertrauen, regionale Spannungen).

Workflow-Zuordnung. SIFT (Archiv; Quellensichtung); 10 Minuten (Kontoverlauf; plattformübergreifende Überprüfungen; früheste Auftritte); 30 Minuten ABCDE (Akteur/Verhalten = Botnets + Trollseiten; Grad = Reichweite/Geschwindigkeit; Effekt = Gemeinschaftsrisiko) → Antwortmatrix und Prebunking.

Was ich lehren soll. Verbinden Sie Punkte aus Beiträgen → vernetzen Sie → Erzählung → Schaden und wählen Sie dann die am wenigsten verstärkende effektive Reaktion aus.

Lesen Sie mehr. Debunk.org Untersuchung(en) und Follow-ups zu Bot-Netzwerken und Zielthemen.

Länder-Playbooks

Der Zweck dieser Länder-Playbooks besteht darin, Methoden, Quellen und Beispiele für jeden Zielkontext zu lokalisieren. Wir wählten die Länder aus, in denen die Aktivitäten dieses Projekts durchgeführt wurden - Österreich, Kroatien und Litauen.

Jedes Playbook enthält die 10 wichtigsten maßgeblichen Quellen (Datenportale von Regierungen/Behörden, Faktencheck-Partner), gängige Narrative und saisonale Zyklen (z. B. Wahlen, Energie, Migration, öffentliche Gesundheit), lokale Plattformmuster (Messaging-Apps vs. offene Netzwerke, Sprachvarianten), rechtliche / Compliance-Besonderheiten (Daten, Medien, Zeitfenster für die Stille von Wahlen) und drei lokale Fallvignetten mit fertigen Übungen.

Litauen (LT)

Die wichtigsten maßgeblichen Quellen (für schnelle Verlinkungen):

- Offizielle Statistik: Statistics Lithuania / Staatliche Datenagentur (OSP-Portal) – www.osp.stat.gov.lt
- Wahlen: Zentrale Wahlkommission (VRK). – www.vrk.lt
- Gesundheit: Gesundheitsministerium (SAM) - www.sam.lrv.lt
- Cybersicherheit: Nationales Zentrum für Cybersicherheit (NCSC) – www.nksc.lt
- Faktencheck/OSINT-Referenzen: Debunk.org (regionale Analysen) – www.debunk.org

Gemeinsame Narrative und saisonale Zyklen: Grenz-/Migrationsereignisse; Energie-/Preisschocks; NATO-Präsenz; Gerüchte aus der Wahlperiode; Die Gesundheitspolitik macht Angst. Verwenden Sie Prebunk-Vorlagen, wenn VRK-Kalender Meilensteine veröffentlichen.

Watchpoints & Plattformmuster: geklonte Mediendomains und Artikel im Doppelgänger-Stil; geoblockierte Weiterleitungen; Facebook/Telegram-Crossposting. Führen Sie Domain-/TLS-/WHOIS-Prüfungen + umgekehrtes Bild (Lens/TinEye) für wiederverwendete visuelle Elemente durch.

Rechtliches/Compliance-Hinweise: VRK-Seiten auf aktuelle Wahlinformationen überprüfen, bevor Korrekturen veröffentlicht werden; Archivieren (Wayback/Perma) aller Links, die in einer Prüfung verwendet werden.

Kroatien (HR)

Top-maßgebliche Quellen:

- Offizielle Statistik: Kroatisches Amt für Statistik (DZS) – www.dzs.gov.hr
- Wahlen: Staatliche Wahlkommission (DIP/SEC) - www.izbori.hr
- Gesundheit: Gesundheitsministerium – www.zdravlje.gov.hr

- Cybersicherheit: Nationales CERT (CERT.hr / CARNET) - www.CERT.hr

Gemeinsame Narrative und saisonale Zyklen: EU-Themen (Schengen/Euro), Migrationsrouten, Energie/Tourismus, Gerüchte über die Wahlsaison. Rechnen Sie mit Copy-Paste-Bursts auf Facebook-Seiten und -Portalen.

Watchpoints & Plattformmuster: Typosquats nationaler Outlets; Telegram/FB-Gruppen recyceln alte Fotos mit neuen Bildunterschriften. Verwenden Sie einen 10-Minuten-Ablauf: Keyframes → Rückwärtssuche; Überprüfung des Domain-Alters/TLS.

Hinweise/Compliance-Hinweise: Verwenden Sie SEC-Seiten für Verfahren und Zeitpläne, wenn Behauptungen die Abstimmung oder die Wahlbeteiligung betreffen; Archivieren Sie Screenshots mit Zeitstempeln, falls Beiträge gelöscht werden.

Österreich (AT)

Top-maßgebliche Quellen:

- Amtliche Statistik: STATISTIK AUSTRIA - www.statistik.at
- Wahlen: Bundeswahlbehörde über das Innenministerium - www.bmi.gv.at
- Gesundheit: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz. - www.sozialministerium.gv.at
- Cybersicherheit: CERT.at (nationales CERT) - www.cert.at

Gemeinsame Narrative und saisonale Zyklen: Energiepreise und Klimapolitik; EU-Verordnung; Migration; grenzüberschreitende Geschichten mit DE/IT/CZ. Geklonte Seiten täuschen manchmal Ministerien oder nationale Rundfunkanstalten vor.

Watchpoints & Plattformmuster: Weiterleitungsketten und Anzeigenplatzierungen auf ähnlich aussehenden Nachrichtenseiten; lokale Facebook-Gruppen, die Screenshots von deutschen Seiten teilen. Überprüfen Sie zuerst die Herkunft der Quelle; Ordnen Sie das Verhalten (Klone/Anzeigen/Weiterleitungen) zu, bevor Sie über den Inhalt diskutieren.

Hinweise: Wahlinformationen sind zentralisiert – Link zu den Seiten der Bundeswahlbehörde für Regeln und offizielle Mitteilungen.

Schlussfolgerung

Dieses Toolkit verwandelt gute Absichten in zuverlässige Übungen. Durch die Kombination klarer Konzepte mit den 5/10/30-Workflows, der ABCDE-Triage und einer disziplinierten Ethik- und Archivierungsroutine bieten wir jedem Botschafter einen wiederholbaren Weg von "das sieht verdächtig aus" zu einer transparenten, verhältnismäßigen Reaktion. Die Tools und Techniken – Quellentriage, visuelle und akustische Verifizierung, Domain-Forensik, OSINT-Geo-/Chrono-Prüfungen und Erkennung von Kampagnenmustern – sind bewusst einfach zu starten und rigoros genug, um in der Öffentlichkeit zu bestehen. Europäische Fallstudien, Länder-Playbooks und Quick Cards übersetzen Methoden in das Muskelgedächtnis, damit Teams schnell handeln können, ohne den Schaden zu verstärken.

Was am wichtigsten ist, ist Konsistenz und Sorgfalt. Führen Sie mit der Wahrheit, zeigen Sie Ihre Methode und Unsicherheit und wählen Sie den am wenigsten verstärkenden Kanal, der die Menschen dennoch schützt. Erfassen Sie Originale, archivieren Sie Links und hinterlassen Sie eine Spur, die ein Kollege morgen reproduzieren kann. Verwenden Sie die Verletzlichkeitslinse, um den Ton und das Timing zu formen. Wenden Sie die Antwortmatrix an, um Maßnahmen und Risiken abzugleichen. und messen Sie, was Sie tun, mit schlanken KPIs, damit sich die Qualität von Monat zu Monat verbessert. Mit der Weiterentwicklung von Plattformen, Taktiken und KI ist auch dieses Toolkit so konzipiert, dass es sich weiterentwickelt: Fügen Sie neue Fälle hinzu, aktualisieren Sie Ihre Schnellkarten, aktualisieren Sie Länderblätter und führen Sie regelmäßige Übungen durch. Wenn wir gemeinsam weiter lernen – und unsere Arbeit nachvollziehbar, respektvoll und klar halten – stärken wir das Vertrauen in unsere Gemeinschaften und erschweren es der Manipulation, sich durchzusetzen.

Anhänge

Glossar

ABCDE Framework — Actor, Behaviour, Content, Degree, Effect — eine strukturierte Methode zur Analyse von Operationen.
Beispiel: Kartieren Sie das Netzwerk (Akteur), die Koordination (Verhalten), die Narrative (Inhalt), die Reichweite (Grad) und die Wirkung (Wirkung).

Archivierung (Wayback, Memento) – Speichern von Schnappschüssen von Webseiten, um Beweise zu sichern und Änderungen zu vergleichen.
Beispiel: Wayback zeigt an, dass die Überschrift nach der Veröffentlichung bearbeitet wurde.

Attribution – Beurteilung, wer wahrscheinlich hinter einer Operation steckt; oft unter Vorbehalt und evidenzbasiert.
Beispiel: Sprachmuster und Hosting verknüpfen eine Website mit einer bekannten einflussreichen Firma.

Bias & Heuristiken – Kognitive Abkürzungen (Bestätigung, Verfügbarkeit, motiviertes Denken), die das Urteilsvermögen verzerren.
Beispiel: Du bemerkst bevorzugt Beispiele, die zu deinen früheren Überzeugungen passen.

Bot/Automatisierung – Konten, die Inhalte automatisch posten oder in unnatürlichem Umfang verstärken.
Beispiel: Ein Profil postet alle 2 Minuten, 24/7, in mehreren Sprachen.

Chain of Custody – Dokumentation, wie Beweise erlangt und gespeichert wurden, um die Integrität zu wahren.
Beispiel: Aufzeichnen der Download-Zeit, der URL und des Hashs für ein Video.

Chronolocation: Bestätigung, wann ein Bild/Video aufgenommen wurde, anhand von Sonnenstand, Wetter oder Ereignishinweisen.
Beispiel: Schattenwinkel und ein Wetterarchiv zeigen, dass das Video vom April 2023 stammt.

Behauptung – Eine Aussage, die behauptet, dass etwas wahr oder falsch ist; die Einheit, die Sie überprüfen.
Beispiel: In einem Beitrag heißt es: "Die Stadt hat ab Januar 2026 alle Gasherde verboten."

Kontextkollaps – Wenn Informationen über ihren ursprünglichen Kontext hinaus geteilt werden, wodurch sich ihre Bedeutung ändert.
Beispiel: Eine satirische Schlagzeile, die gepostet wird, als ob es sich um echte Nachrichten handelt.

Koordiniertes unauthentisches Verhalten (CIB) – Organisierte Nutzung gefälschter Konten/Seiten, um über Identität oder Zweck irrezuführen.
Beispiel: Ein Cluster von Seiten teilt täglich zur gleichen Minute identische Beiträge.

Korrektur / Aktualisierung – Eine transparente Notiz, die Fehler behebt oder nach der Veröffentlichung neue Informationen hinzufügt.
Beispiel: "Aktualisiert am 4. Nov. 2025: Datum korrigiert vom 12. Okt. bis 21. Okt."

Querverweis — Bestätigung einer Tatsache durch unabhängige, glaubwürdige Quellen.
Beispiel: Bestätigung von Zahlen über den offiziellen Datensatz und einen separaten Prüfbericht.

Deepfake / Synthetische Medien – Audio-, Bild- oder Videodateien, die von KI generiert oder verändert werden, um reale Personen oder Ereignisse realistisch nachzuahmen.
Beispiel: Eine von der KI geklonte Sprachaufzeichnung, die fälschlicherweise ein Verbrechen "zugibt".

Desinformation – Falsche oder irreführende Informationen, die absichtlich erstellt oder verbreitet werden, um zu täuschen.
Beispiel: Ein Netzwerk von Seiten fabriziert Umfragezahlen, um von der Stimmabgabe abzuhalten.

DSA / Code of Practice — EU-Gesetz über digitale Dienste und freiwilliger Kodex zur Orientierung und Transparenz der Plattformen.
Beispiel: Plattformen veröffentlichen Anzeigenbibliotheken und Risikobewertungen pro DSA.

Beweise – Informationen, die eine Behauptung stützen oder widerlegen. Dabei kann es sich um Dokumente, Daten, Bilder, Videos oder Expertenaussagen handeln.
Beispiel: Ein Abstimmungsprotokoll des Stadtrats und der offizielle Verordnungstext.

Geolokalisierung: Bestätigen, wo ein Bild/Video aufgenommen wurde, indem Orientierungspunkte, Schilder oder Gelände abgeglichen werden.
Beispiel: Identifizieren einer Skyline und von Straßenschildern, um ein Video in Kaunas zu platzieren.

Hash / Prüfsumme – Ein eindeutiger Fingerabdruck einer Datei, um zu beweisen, dass sie sich nicht geändert hat.
Beispiel: MD5/SHA256 stimmt vor und nach der Übertragung überein.

Seitliches Lesen — Öffnen Sie neue Tabs, um zu überprüfen, wer die Quelle ist, bevor Sie genau lesen.
Beispiel: Sie überprüfen zuerst die "Info"-Seite und die externen Profile einer Website.

Fehlinformationen – Echte Informationen, die aus dem Zusammenhang gerissen oder mit schädlichem Framing geteilt werden, um Schaden anzurichten.
Beispiel: Die Privatadresse einer Person preisgeben, um zu Belästigung aufzurufen.

Metadaten / EXIF — Eingebettete technische Daten über eine Datei (Gerät, Zeit, GPS). Oft von Plattformen abgestreift.
Beispiel: Das Originalfoto zeigt GPS-Koordinaten und die Aufnahmezeit.

Fehlinformationen – Falsche oder irreführende Informationen, die ohne Täuschungsabsicht weitergegeben werden.
Beispiel: Ein Freund teilt eine veraltete Karte mit falschen Evakuierungszonen.

Narrativ vs. Behauptung – Eine Erzählung ist eine breitere Geschichte; eine Behauptung ist eine spezifische, überprüfbare Aussage.
Beispiel: Narrativ: "Wahlen sind manipuliert." Behauptung: "10.000 tote Wähler gaben ihre Stimme in Stadt X ab."

OSINT (Open-Source Intelligence) – Sammeln und Analysieren öffentlich zugänglicher Daten zur Überprüfung von Fakten.

Beispiel: Verwendung von Unternehmensregistern und Flugtrackern, um die Reise einer Person zu bestätigen.

Prebunking / Inokulation — Manipulationstaktiken und Gegenargumente lehren, bevor die Menschen darauf stoßen.
Beispiel: Eine Lektion über "falsche Dilemmata" reduziert die spätere Anfälligkeit.

Primärquelle – Originalmaterial, das zum Zeitpunkt eines Ereignisses oder direkt von der Person erstellt wurde.
Beispiel: Das Verordnungs-PDF auf der offiziellen Website der Stadt.

Propagandamittel — Klassische Techniken: Beschimpfungen, glitzernde Allgemeinheiten, Transfer, Zeugnisse, einfache Leute, Kartenstapeln, Zugwagen.
Beispiel: In einer Anzeige wird ein "Testimonial" eines Prominenten ohne Beweise verwendet.

Verhältnismäßigkeit – Abstimmung der Stärke Ihrer Schlussfolgerung mit der Qualität/Quantität der Beweise.
Beispiel: "Nicht überprüft", wenn Quellen in Konflikt stehen; Vermeiden Sie es, zu viel zu beanspruchen.

Zuverlässigkeitskennzeichnungen – Plattform- oder Drittanbieterindikatoren für Verkaufsstellen (z. B. öffentlich-rechtlicher Rundfunk, staatsnah).
Beispiel: In einem Video wird unter dem Kanalnamen das Label "staatlich kontrollierte Medien" angezeigt.

Reverse Image Search – Suche nach früheren oder ursprünglichen Versionen eines Bildes, um Herkunft und Kontext zu überprüfen.
Beispiel: Ein Protestfoto auf eine Veranstaltung aus dem Jahr 2016 zurückführen, nicht auf "heute".

Safety & Harm Assessment — Beurteilung potenzieller Risiken (Privatsphäre, Doxing, Retraumatisierung) vor der Veröffentlichung.
Beispiel: Sie verwischen Gesichter von Minderjährigen in Protestaufnahmen.

Satire / Parodie — Humorvolle oder übertriebene Inhalte, die echte Nachrichten oder Personen imitieren.
Beispiel: Eine Website veröffentlicht einen gefälschten Artikel über Raketenstarts auf der "flachen Erde".

Sekundärquelle: Eine Zusammenfassung, Analyse oder ein Bericht, der auf Primärquellen basiert.
Beispiel: Ein Nachrichtenartikel, der die Verordnung beschreibt und Beamte zitiert.

SIFT-Methode – Stopp, Quelle untersuchen, Bessere Abdeckung finden, Rückverfolgung zum Original.
Beispiel: Bevor Sie retweeten, halten Sie an und suchen die ursprüngliche Pressemitteilung.

Sockenpuppe / Astroturfing – Falsche Identitäten, die Unterstützung von der Basis vortäuschen.
Beispiel: Ein Unternehmen betreibt "Bürger"-Seiten, auf denen es sein Produkt lobt und Kritiker angreift.

Quellentransparenz – Klare Informationen darüber, wer eine Website/ein Konto betreibt, Finanzierung, Korrekturrichtlinien und Kontaktdaten.
Beispiel: Das Outlet listet seine Redaktion und ein Korrekturprotokoll auf.

Truth Sandwich — Kommunikationstaktik: Sagen Sie die Wahrheit → sprechen Sie den Mythos an → bekräftigen Sie die Wahrheit mit Beweisen.
Beispiel: "Impfstoffe sind sicher und wirksam. In einem viralen Beitrag wird fälschlicherweise X behauptet. Hier sind die Daten, die die Sicherheit zeigen."

Verifizierungs-Workflow (10.05.30) – Selektierungstiefe basierend auf der verfügbaren Zeit: 5 Minuten Schnellprüfung, 10 Minuten tiefer, 30 Minuten vollständig.
Beispiel: In 5 Minuten überprüfen Sie die Überschrift, die Quelle und den ursprünglichen Link; In 30 nehmen Sie Kontakt zu Experten auf.

Gefördert durch die Europäische Union. Die geäußerten Ansichten und Meinungen sind jedoch nur die des Autors/der Verfasser und spiegeln nicht unbedingt die Ansichten und Meinungen der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die Bewilligungsbehörde können für sie verantwortlich gemacht werden.