ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

12

BAND

Muster, Beziehungen und Grenzen der Attribuierung

Spanische Ausgabe · 2026

Handbuch zur Analyse von Botnetzwerken, gefälschten Profilen und Medienschäden

Beweissicherung, Chronologie, Indikatoren, Graphen, alternative Hypothesen und technischer Bericht

Koordiniertes Verhalten analysieren, ohne eine Koinzidenz als Beweis für Automatisierung, eine Kontobeziehung als Beweis für Inhaberschaft oder eine unpopuläre Meinung als Beweis für eine Straftat auszugeben.

Für Analysten, Sachverständige, Forschende, juristische Teams sowie Kommunikations-, Reputations- und Compliance-Verantwortliche. Die Erhebung beschränkt sich auf öffentliche oder autorisierte Quellen und umfasst weder die Umgehung von Kontrollen noch Identitätstäuschung oder die Offenlegung von Personen.

Redaktionelle Koordination: Jocsan Laguna · Amerikanischer Rat für Cybersicherheit und digitale Forensik

Allgemeiner technischer Leitfaden und offenes Bildungsmaterial. Er stellt keine Rechtsberatung oder forensisches Gutachten dar und enthält keine Anleitung zum unbefugten Zugriff auf Systeme. Beispiele und Daten sind fiktiv; die Abbildungen sind redaktionelle Rekonstruktionen.

Inhalt

Die sichtbare Seitennummerierung entspricht der PDF-Ausgabe. Word kann dieses Inhaltsverzeichnis beim Öffnen des Dokuments aktualisieren; die Überschriften ermöglichen weiterhin die interne Navigation.

Einleitung: Viele Konten bedeuten nicht eine einzige Person 3
Kapitel 1. Fragestellung und Kriterien 3
1.1 Aussagen, die unterschiedliche Beweise erfordern 3
1.2 Hypothesen und Falsifikation 4
Kapitel 2. Sicherung der Ausgangslage 4
2.1 Objekte, die verschwinden können 4
2.2 Beziehungen und Abfolge 4
2.3 Datenschutz und Verhältnismäßigkeit 5
Kapitel 3. Inhalt und Chronologie 6
3.1 Text, Varianten und frühe Quelle 6
3.2 Zeitfenster und Häufigkeit 6
3.3 Links und Parameter 7
Kapitel 4. Koordination und Hypothesen 7
4.1 Konvergierende Indikatoren 7
4.2 Alter, Veränderungen und Community 7
4.3 Bewertung der Automatisierung 8
Kapitel 5. Graphen und Infrastruktur 9
5.1 Ein Knoten ist keine Person 9
5.2 Domains, IP und gemeinsam genutzte Dienste 9
5.3 Attribuierungsskala 9
Kapitel 6. Medienschaden und Bericht 10
6.1 Ausmaß und Folgen 10
6.2 Reproduzierbarer technischer Bericht 10
6.3 Anschließende Maßnahmen 10
Anhang A. Analyseformate 11
A.1 Inventar der Konten und Inhalte 11
A.2 Indikatorenmatrix 11
A.3 Berichtsstruktur 12
A.4 Aufzeichnung etwaiger Simulationen 12
Anhang B. Rechtsrahmen und Abschlusskontrolle 12

Einleitung: Viele Konten bedeuten nicht eine einzige Person

Ein Dutzend Profile, die denselben Text veröffentlichen, kann wie eine zentral gesteuerte Operation wirken. Es kann sich ebenso um eine Community handeln, die eine Vorlage, eine dringende Nachricht oder ein berechtigtes Anliegen teilt. Die Analyse beginnt damit, die naheliegende Schlussfolgerung zu vermeiden: Sie beschreibt die Handlungen der Konten, ihre Abfolge und Beziehungen sowie andere Erklärungen, die dasselbe Muster erzeugen könnten.

„Bot“, „gefälschtes Profil“, „koordiniertes Konto“, „Troll“, „Farm“ und „Einflussoperation“ sind keine Synonyme. Ein Konto kann automatisiert sein, ohne koordiniert zu sein; mehrere Personen können sich ohne Automatisierung koordinieren; ein Profil kann einen fiktiven Namen verwenden, ohne in jeder Hinsicht falsch zu sein; eine Kampagne kann wahrheitsgemäße Inhalte und zugleich täuschendes Verhalten aufweisen. Der Bericht definiert seine Kategorien und weist sie jeweils gesondert nach.

Die Analyse muss keine Schlagzeile erfinden, um nützlich zu sein. Sie kann nachweisen, dass eine Gruppe von Konten Text, Zeitfenster, Links, Abfolge und Beziehungen in einem im Vergleich zu einer dokumentierten Referenz auffälligen Maße teilt. Gemeinsame Infrastruktur kann Indizien liefern, aber eine IP-Adresse oder eine Domain macht nicht alle Konten zu ein und derselben Person. Die Attribuierung endet dort, wo die Quelle endet.

> **Leitgrundsatz**
> Zuerst Muster und Abdeckung, dann alternative Erklärungen und erst am Ende der Grad an Attribuierung, den das Beweismaterial tatsächlich trägt.

Kapitel 1. Fragestellung und Kriterien

1.1 Aussagen, die unterschiedliche Beweise erfordern

Fünf Fragen werden getrennt: welche Inhalte veröffentlicht wurden, welche Konten beteiligt waren, welches Verhalten sie zeigen, welche Beziehungen bestehen und wer sie kontrolliert. Die ersten Fragen lassen sich mit Beiträgen und Aufzeichnungen beantworten; Koordination erfordert Vergleiche; Inhaberschaft erfordert eine andere Art von Quelle. Ohne diese Unterscheidung behauptet eine ansprechende Grafik am Ende mehr als die Untersuchung belegt.

Der Untersuchungsumfang umfasst Plattform, Zeitraum, Zeitzone, Ausgangskonten, Suchbegriffe, Inhaltstyp, Datenquellen und Ausschlüsse. Dokumentiert wird, wie die Stichprobe gefunden wurde: Suche, vorhandene Liste, API, Export, Verweise oder manuelle Auswahl. Eine Auswahl nach dem Grad der Empörung erzeugt eine verzerrte Stichprobe. Wer nur virale Beiträge erfasst, vergleicht nicht mit dem gewöhnlichen Verhalten.

Aussage	Erforderliches Beweismaterial	Nicht automatisch daraus ableiten
Identischer Inhalt	Text, Version, URL, Datum und frühe Quelle.	Einen einzigen Autor oder eine zentrale Veröffentlichungsstelle.
Gleichzeitigkeit	Zeitzone, vorhandene Sekundenangaben und vollständige Abfolge.	Automatisierung allein aufgrund zeitlicher Nähe.
Koordination	Mehrere Indikatoren und Vergleich mit einer Referenz.	Koordination aufgrund einer einzigen Koinzidenz.

Aussage	Erforderliches Beweismaterial	Nicht automatisch daraus ableiten
Automatisierung	Technische Muster, Aktivität und verfügbare Kontrollen.	Dass jedes repetitive Verhalten ein Bot sei.
Kontoinhaberschaft	Kontrollaufzeichnungen und rechtliche Bestätigung.	Eine bestimmte Person allein aufgrund von Foto, IP oder Name.
Schaden	Inhalt, Reichweite, Kontext und nachgewiesene Folgen.	Die Gesamtwirkung allein aus Impressionen.

1.2 Hypothesen und Falsifikation

Eine Ausgangshypothese könnte lauten: „Die Konten A–H handeln koordiniert, um Inhalt X zu verstärken.“ Eine Alternative könnte sein: „Unabhängige Nutzer teilen aufgrund eines externen Ereignisses eine Vorlage.“ Eine weitere könnte lauten: „Die Plattform erzeugt durch ihre Empfehlungsreihenfolge ein scheinbares Muster.“ Jede Hypothese erfordert eine Prüfung, die sie schwächen kann: frühe Quelle, Textvarianten, vorherige Abfolge, Verhalten außerhalb des Ereignisses und Vergleich mit anderen Gruppen.

Die Referenz wird vor der Berechnung festgelegt. Es kann sich um eine andere Diskussion zum selben Thema, einen anderen Zeitraum derselben Konten oder eine vergleichbare Nutzergruppe handeln. Ein Schwellenwert wird nicht deshalb gewählt, weil er das gewünschte Ergebnis liefert. Fehlt eine geeignete Referenz, wird die Auffälligkeit als beschreibend ausgewiesen und keine erfundene Wahrscheinlichkeit zugewiesen.

> **Beweisgrundsatz**
> Eine gute Untersuchung sucht nicht nur nach weiteren Indizien für Koordination. Sie sucht auch nach Daten, die zeigen könnten, dass die ursprüngliche Erklärung nicht erforderlich ist.

Kapitel 2. Sicherung der Ausgangslage

2.1 Objekte, die verschwinden können

Beiträge, Profile, Biografien, Bilder, Antworten, Zitate, Reposts, Links, Kennzahlen, Daten und sichtbare Änderungen werden gesichert. Jedes Objekt erhält eine Kennung und wird mit URL, Konto, Plattform, Datum und Erfassungsmethode verknüpft. Ein Screenshot einer Startseite beweist weder alle Beiträge eines Kontos noch den früheren Zustand eines Netzwerks.

Bei einem autorisierten Export oder einer autorisierten API werden Endpunkt oder Funktion ohne Geheimnisse, Version, Parameter, Filter, Paginierung, Grenzen, Zeitzone, Format, Datum und Fehler dokumentiert. Die erhaltenen Daten werden im nativen Format und, sofern vorhanden, mit einem Datenwörterbuch aufbewahrt. Bei einer ausschließlich manuellen Erfassung werden die erfassende Person, ihre Rolle und der Umfang der Prüfung vermerkt. Zugangsbeschränkungen werden nicht umgangen, um den Datensatz zu vervollständigen.

2.2 Beziehungen und Abfolge

Beziehungen werden als separate Objekte erfasst: Konto A antwortet B, zitiert C, teilt Link D oder folgt E. Der Inhalt, der jede Kante belegt, und das sichtbare Datum werden aufbewahrt. Ein Graph ohne diese Referenzen kann ansprechend aussehen und dennoch nicht überprüfbar sein. Die Richtung der Beziehung ist wichtig: Folgen ist nicht dasselbe wie gefolgt zu werden, und Zitieren ist nicht dasselbe wie Verfassen des ursprünglichen Textes.

Die Chronologie hält das Datum im Wortlaut, die Zeitzone, die Genauigkeit und die Bedeutung fest: Erstellung, Bearbeitung, Veröffentlichung, Erfassung und Messung sind unterschiedliche Ereignisse. Plattformen können nach Relevanz statt nach Zeit sortieren. Die Abfolge wird nach Möglichkeit anhand von Beitragskennungen und externen Quellen rekonstruiert, ohne die Bildschirmreihenfolge mit der tatsächlichen Reihenfolge gleichzusetzen.

Objekt	Mindestaufzeichnung	Grenze
Beitrag	URL, ID, Konto, Text, Medien und Datum.	Nicht der vollständige Kontext des Kontos.
Profil	URL, angezeigter Name, Biografie und Änderungen.	Weder tatsächliche Inhaberschaft noch automatisch bestimmter Standort.
Beziehung	Ursprung, Typ, Ziel und Beweismaterial.	Keine Aussage über Kontrollrichtung oder Absicht.
Kennzahl	Wert, Datum, Bedeutung und Plattform.	Weder einzelne Leser noch der Gesamtschaden.
Export	Parameter, Abdeckung, Filter und Datenwörterbuch.	Keine Aussage über Vollständigkeit außerhalb der Abfrage.
Erfassung	Erfassende Person, Rolle, Datum und Umfang.	Ersetzt nicht ein verfügbares natives Format.

2.3 Datenschutz und Verhältnismäßigkeit

Die Untersuchung von Profilen kann Personen offenlegen, die mit dem Schaden nichts zu tun haben. Die Erhebung wird auf das Erforderliche beschränkt; Arbeits- und Veröffentlichungsversion werden getrennt. Personenbezogene Daten werden nicht veröffentlicht, um eine Hypothese angeblich zu beweisen. Auf private Profile wird nicht durch Identitätstäuschung oder falsche Konten zugegriffen; stattdessen wird ein autorisierter Weg angefordert oder die Einschränkung ausgewiesen.

> **Sicherheitsgrundsatz**
> Eine Untersuchung von Medienschäden darf nicht selbst weiteren Schaden verursachen. Der Bericht kann Beziehungen nachweisen, ohne Adressen, Telefonnummern, Angaben zu Minderjährigen, Fotografien oder unbelegte mutmaßliche Identitäten zu veröffentlichen.



Abbildung 1. Das Netzwerk wird gesichert, bevor es verschwindet. Objekt, Beziehung, Zeitpunkt und Abdeckung. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 3. Inhalt und Chronologie

3.1 Text, Varianten und frühe Quelle

Der Text wird im Wortlaut und in seinen Varianten verglichen: Wörter, Hashtags, gemeinsame Fehler, Leerzeichen, Links, Emojis, Formatierung und Ausschnitte. Eine öffentliche Vorlage kann Übereinstimmungen erklären; ein seltener Fehler kann auf eine gemeinsame Quelle hindeuten, identifiziert aber nicht deren Autor. Die früheste Version wird gesucht, und es wird vermerkt, ob eine noch frühere Version außerhalb des Untersuchungsumfangs existiert haben könnte.

Bilder und Videos können dieselbe Datei, Kennzeichnung, denselben Ausschnitt oder dieselben Metadaten aufweisen. Dieselbe Datei in zwei Konten beweist keine Koordination, wenn es sich um ein verbreitetes oder von einer Organisation bereitgestelltes Bild handelt. Untersucht wird, wer die Datei innerhalb des Datensatzes zuerst veröffentlichte, wie sie verändert wurde und ob die Konten verwandte Linkparameter oder Namen verwendeten. Die Authentizität der dargestellten Szene wird mit anderen Methoden bewertet.

3.2 Zeitfenster und Häufigkeit

Gleichzeitigkeit benötigt Einheiten und eine Referenz. Was bedeutet „zur gleichen Zeit“: dieselbe Sekunde, Minute, Stunde oder derselbe Tag? Eine dringende Nachricht kann Tausende zeitlich nahe Beiträge auslösen. Die Verteilung wird unter Angabe von Zeitzone und Genauigkeit mit früheren Zeiträumen und anderen Diskussionen verglichen. Ein Zeitfenster wird nicht nachträglich deshalb gewählt, weil es genau die verdächtigen Konten zusammenfasst.

Die Veröffentlichungshäufigkeit kann auf Automatisierung oder ein Team hindeuten, aber ebenso auf eine geplante Kampagne oder eine sehr aktive Person. Pausen, Regelmäßigkeit, Vielfalt der Inhalte und Tageszeiten werden im Kontext analysiert. Ein Konto, das 24 Stunden lang veröffentlicht, ist nicht automatisch ein Bot: Es kann von Personen in mehreren Zeitzonen verwaltet werden.

3.3 Links und Parameter

Links werden nach Domain, Pfad, Weiterleitung, Parametern, Kampagne, gegebenenfalls öffentlich zugänglichem Registrierungsdatum und Beziehung zu anderen Objekten analysiert. Ein identischer Parameter kann auf das Kopieren desselben Links, eine Vorlage oder eine gemeinsame Konfiguration hindeuten; er beweist keine gemeinsame Inhaberschaft. Die Abfolge der Weiterleitungen und der abschließende Inhalt werden gesichert, ohne gefährliche Ziele in einer Produktivumgebung aufzurufen.

Indiz	Legitime alternative Erklärung	Prüfung
Derselbe Textfehler	Gemeinsam genutzte Vorlage oder gemeinsames Zitat.	Frühe Quelle und Varianten zwischen den Konten.
Zeitlich nahe Veröffentlichungen	Dringende Nachricht oder geplantes Ereignis.	Referenzverteilung und früheres Verhalten.
Derselbe Link	Verbreitete Quelle oder öffentliche Kampagne.	Parameter, erste Verwendung und Weiterleitungen.
Dasselbe Bild	Kommunikationsmaterial oder Trend.	Datei, Version, Bildausschnitt und Erstveröffentlichung.
Kontinuierliche Aktivität	Schichtarbeit, Zeitplanung oder intensive Nutzung.	Handlungstypen, Zeitzonen und verfügbare Protokolle.

Fiktiver Fall

Acht Konten veröffentlichen denselben Link innerhalb von zwei Minuten. Die Referenz zeigt, dass Tausende ihn aufgrund einer Nachricht teilen. Jedoch verwenden nur diese acht denselben seltenen Parameter und denselben Textfehler, und sie waren bereits zuvor gemeinsam aktiv. Die Koordination gewinnt durch das Zusammentreffen mehrerer Indizien an Stütze, nicht durch die zwei Minuten.

Kapitel 4. Koordination und Hypothesen

4.1 Konvergierende Indikatoren

Eine Matrix wird mit Inhalt, Zeit, Links, Verlauf, Beziehungen, Profiländerungen, früherem Verhalten und möglichen externen Quellen erstellt. Für jeden Indikator werden eine alternative Erklärung und eine Prüfung festgelegt. Die Beweiskraft wird nicht durch einfaches Zählen der Signale bestimmt: Einige sind voneinander abhängig, andere können auf der Plattform häufig vorkommen.

Die Referenz ermöglicht die Aussage, ob eine Häufigkeit oder Beziehung atypisch ist. Die Intervallverteilung kann mit früheren Zeiträumen oder mit kontrollierten Permutationen der Daten verglichen werden, wobei relevante Merkmale erhalten bleiben. Bei einer Simulation werden Seed, Regeln, Annahmen und Anzahl der Iterationen dokumentiert. Eine statistische Wahrscheinlichkeit wird nicht ausgewiesen, wenn das Modell den tatsächlichen Prozess nicht abbildet.

4.2 Alter, Veränderungen und Community

Viele neue Konten können durch eine Plattformmigration oder eine Einladungskampagne entstehen. Die Erstellungsdaten werden als Gruppe analysiert und mit der Aktivität davor und danach verglichen. Gleichzeitige Änderungen von Name, Bild oder Beschreibung können auf eine Vorlage, aber auch auf ein Community-Ereignis hindeuten. Der sichtbare Verlauf wird gesichert, bevor er verschwindet.

Gegenseitiges Folgen kann auf ein Netzwerk oder schlicht auf eine gleichgesinnte Community hindeuten. Die Verbindungsdichte wird mit anderen Gruppen verglichen, ebenso Gegenseitigkeit, Aktivität außerhalb der Gruppe und frühere Beziehungen. Dichte beweist keine zentrale Kontrolle. Eine kleine

Gruppe kann stark verbunden sein, weil sich ihre Mitglieder kennen; der Graph muss durch Inhalt und Chronologie ergänzt werden.

4.3 Bewertung der Automatisierung

Die Bewertung der Automatisierung stützt sich auf technisches Verhalten: repetitive Handlungen in Intervallen, Schnittstellennutzung, Inhaltsmuster, unmittelbare Reaktionen und eine Kontinuität, die mit vertretbarer menschlicher Aktivität unvereinbar ist. Dennoch gibt es legitime Planungswerkzeuge und menschliche Teams mit Routinen. Der Bericht kann „mit Automatisierung vereinbares Verhalten“ feststellen, ohne ein bestimmtes Werkzeug zu behaupten, wenn keine Protokolle vorliegen.

Dimension	Frage	Grenze der Schlussfolgerung
Inhalt	Gibt es Varianten oder nur wörtliche Kopien?	Eine Vorlage bedeutet keine zentrale Kontrolle.
Zeit	Ist das Muster im Vergleich zur Referenz atypisch?	Gleichzeitigkeit bedeutet nicht, dass ein Bot vorliegt.
Verlauf	Bestand die Koordination bereits vor dem Ereignis?	Neue Konten können durch eine Migration entstanden sein.
Beziehungen	Ist die Dichte höher als in einer vergleichbaren Community?	Freundschaft und Gemeinsamkeiten erzeugen ebenfalls dichte Graphen.
Schnittstelle	Gibt es Beweise für Automatisierung?	Legitime Zeitplanung ist möglich.
Attribuierung	Welche Quelle belegt die tatsächliche Kontrolle?	Eine IP oder ein Bild genügt nicht.

Belastbare Schlussfolgerung

„Die Gruppe weist Übereinstimmungen bei Inhalt, Parametern, Abfolge und früherem Verhalten auf, die mit Koordination vereinbar sind. Die Abdeckung erlaubt weder die Attribuierung an eine Person noch an ein bestimmtes Werkzeug.“



Abbildung 2. Koordination wird anhand alternativer Erklärungen geprüft. Konvergierende Indikatoren statt eines einzelnen spektakulären Signals. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 5. Graphen und Infrastruktur

5.1 Ein Knoten ist keine Person

Je nach Legende stellt ein Knoten ein Konto, einen Beitrag, einen Link oder eine Infrastruktur dar. Die Kante stellt eine dokumentierte Beziehung dar, keine Anweisung. Der Graph muss Typ, Richtung, Zeitraum, Quelle und Abdeckung enthalten. Werden Knoten algorithmisch gruppiert, werden Methode und Parameter dokumentiert; ein Cluster wird ohne qualitative Validierung nicht als reale Organisation dargestellt.

Ein zentrales Konto kann schlicht eine verbreitete Quelle sein. Eine Brücke zwischen Gruppen kann ein Medium oder eine Person sein, die allen antwortet. Zentralitätskennzahlen geben Hinweise für die Prüfung, beweisen aber keine Kontrolle. Der Bericht enthält die Kantenliste, damit andere nachvollziehen können, warum zwei Knoten verbunden sind.

5.2 Domains, IP und gemeinsam genutzte Dienste

Eine IP-Adresse kann zu einer Plattform, einem VPN, einem Unternehmen, einem gemeinsam genutzten Haushalt oder einem Dienst mit dynamischer Vergabe gehören. Eine Domain kann Hosting, DNS oder ein Zertifikat mit Tausenden Websites teilen. Gemeinsame Infrastruktur kann Anfragen und Analysen orientieren, belegt aber keine gemeinsame Inhaberschaft der Konten. Sie wird nicht zur Geolokalisierung von Personen verwendet.

Erforderliche technische Protokolle werden über einen rechtlich zulässigen Kanal angefordert. Es werden weder intrusive Scans durchgeführt noch Datenbanken mit kompromittierten Zugangsdaten durchsucht, um Konten zu verknüpfen. Bei öffentlichen Quellen werden Datum und Abdeckung dokumentiert. Ein Datenleck berechtigt nicht zum Herunterladen, Zusammenführen oder Veröffentlichen personenbezogener Daten.

5.3 Attribuierungsskala

Ebene	Zulässige Aussage	Nicht daraus ableitbar
Inhalt	Diese Beiträge und Versionen waren vorhanden.	Dass das geschilderte Ereignis tatsächlich stattgefunden hat.
Verhalten	Diese Handlungen weisen ein Muster auf.	Dass das Konto ein Bot ist.
Beziehung	Die Konten interagieren auf diese Weise.	Dass sie sich gegenseitig kontrollieren.
Infrastruktur	Sie nutzen denselben Dienst oder dieselben Parameter.	Dieselbe Inhaberschaft oder derselbe Standort.
Koordination	Konvergierende Indizien, die mit Koordination vereinbar sind.	Steuerung durch eine Person.
Kontoinhaberschaft	Durch zulässige Quellen und Kontext belegte Kontrolle.	Keine Ableitung aus Name, Foto oder IP.

Berufliche Grenze

Der Bericht kann hinsichtlich der Koordination belastbar und hinsichtlich der Urheberschaft zurückhaltend sein. Er muss nicht klären, wer dahintersteht, um nachzuweisen, wie sich das Netzwerk verhalten hat.

Kapitel 6. Medienschaden und Bericht

6.1 Ausmaß und Folgen

Inhalt, Verhalten, sichtbare Reichweite und nachgewiesene Folgen werden getrennt betrachtet. Impressionen entsprechen nicht einzelnen Lesern, Reaktionen nicht Zustimmung und Kommentare beweisen keine Meinungsänderung. Der Bericht erfasst Kennzahlen mit Datum und bekannter Bedeutung, ohne daraus eine allgemein gültige Schadensgröße abzuleiten.

Der Schaden wird anhand von Kommunikation, arbeitsbezogenen Entscheidungen, Verträgen, Zeugenaussagen, Meldungen, Betreuung Betroffener und anderen Quellen dokumentiert. Nicht alles, was nach der Kampagne geschieht, wird ohne Prüfung anderer Ursachen dieser Kampagne zugeschrieben. Die Sicherung belegt das Vorhandensein eines Musters; Kausalität erfordert zusätzlich eine Abfolge und weiteres Beweismaterial.

6.2 Reproduzierbarer technischer Bericht

Der Bericht enthält Auftrag, Untersuchungsumfang, Quellen, Methode, Datenwörterbuch, Chronologie, Indikatoren, Referenz, Graph, alternative Erklärungen, Feststellungen, Einschränkungen und Anhänge. Objektkennungen und Abfragen werden veröffentlicht, damit die Analyse wiederholt werden kann. Aussagen über Verhalten werden mit Beiträgen und Aussagen über Auswirkungen mit konkreten Dokumenten verknüpft.

Die öffentliche Version kann Konten oder Daten auslassen, die zum Verständnis der Methode nicht erforderlich sind, ohne die Begründung zu verschleiern. Ändert sich eine Aussage, wenn ein Beitrag entfernt wird, wird ihre Belastbarkeit überprüft. Fehlt der Zugriff auf private Inhalte oder Plattformprotokolle, wird die Abdeckung ausgewiesen. Lücken werden nicht durch Spekulation geschlossen.

6.3 Anschließende Maßnahmen

Die Meldung an die Plattform benennt Inhalt, Konten, Muster und Beweismaterial; eine öffentliche Anschuldigung ist kein Ersatz dafür. Anträge auf Entfernung oder Sicherung werden mit Datum und Vorgangsnummer dokumentiert. Die Kommunikation mit Betroffenen vermeidet eine Wiederholung des schädlichen Inhalts und erklärt die laufenden Maßnahmen. Bei Drohungen oder körperlicher Gefahr hat der örtliche Notfallkanal Vorrang.

Die Verordnung über digitale Dienste regelt Vermittlungsdienste und systemische Risiken bestimmter sehr großer Plattformen. Die Verordnung (EU) 2024/900 behandelt Transparenz und Targeting politischer Werbung, mit Grenzen für spontane Inhalte. Beide gelten nicht automatisch für jedes Konto oder jedes Land und machen Desinformation nicht zu einem allgemein gültigen Tatbestand der Rechtswidrigkeit.[1][2]

> **Abschluss**
> Der Bericht soll ein Verhalten und seine Grenzen verständlich machen, nicht eine neue unbewiesene Anschuldigung erzeugen. Das Beweismaterial wird über den geeigneten Kanal übergeben, nicht durch öffentliche Bloßstellung verbreitet.

[1] Verordnung (EU) 2022/2065 über digitale Dienste. Regelungen für Vermittlungsdienste, Management systemischer Risiken bei bestimmten sehr großen Plattformen und Suchmaschinen sowie Inhaltsregeln. Sie macht nicht aus jedem Muster einen Beweis für Koordination oder aus jeder Meinung rechtswidrige Inhalte. Offizielle Online-Quelle

[2] Verordnung (EU) 2024/900 über Transparenz und Targeting politischer Werbung. Besondere Regeln für politische Werbedienste und damit verbundene Risiken; sie gilt nicht undifferenziert für alle spontanen Inhalte von Nutzern. Offizielle Online-Quelle



Abbildung 3. Der Bericht trennt Muster, Infrastruktur und Person. Die Schlussfolgerung geht nicht über die Aussagekraft der Quelle hinaus. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Anhang A. Analyseformate

A.1 Inventar der Konten und Inhalte

Feld	Erforderliche Aufzeichnung	Kontrolle
Konto / URL	Kennung, Plattform, Profil und Beobachtungsdatum.	Keinen vermuteten Personennamen.
Beitrag	ID, Text, Version, Medien und Datum im Wortlaut.	Gesichertes Objekt.
Beziehung	Ursprung, Typ, Ziel und Beweismaterial.	Keine Kontrolle ableiten.
Zeit	Zeitzone, Genauigkeit und Bedeutung.	Erstellung und Erfassung nicht vermischen.
Kennzahl	Wert, Datum und Bedeutung auf der Plattform.	Keine einzelnen Leser.
Abdeckung	Abfrage, Filter, Zugriff und fehlende Daten.	Keine Vollständigkeit behaupten.
Datenschutz	Sensible Daten, Beschränkungen und öffentliche Version.	Tatsächliche Datenminimierung.

A.2 Indikatorenmatrix

Indiz	Alternative	Prüfung	Begrenztes Ergebnis
Text / gemeinsamer Fehler	Vorlage oder Zitat.	Frühe Quelle und Varianten.	[ ]
Enges Zeitfenster	Nachricht oder Ereignis.	Referenz und frühere Verteilung.	[ ]

Indiz	Alternative	Prüfung	Begrenztes Ergebnis
Linkparameter	Kopie oder öffentliche Kampagne.	Erste Verwendung und Weiterleitungen.	[ ]
Gemeinsames Kontenalter	Migration oder Ereignis.	Frühere Aktivität und Kontext.	[ ]
Dichter Graph	Gleichgesinnte Community.	Referenz und Verhalten außerhalb der Gruppe.	[ ]
Gemeinsame Infrastruktur	Gemeinsamer Anbieter.	Registrierung und andere Konten.	[ ]

A.3 Berichtsstruktur

Praktischer Aufbau

```
1. Auftrag, Fragen, Untersuchungsumfang und Ausschlüsse
2. Quellen, Abdeckung, Datenwörterbuch und Einschränkungen
3. Sicherung und Objektmanifest
4. Chronologie und Inhaltsvarianten
5. Koordinationsindikatoren und Referenz
6. Beziehungen und Graph mit überprüfbaren Kanten
7. Alternative Hypothesen und negative Ergebnisse
8. Sichtbare Reichweite und nachgewiesene Folgen
9. Schlussfolgerungen nach Attribuierungsgrad
10. Datenschutz, Übergabe, Anhänge und Version
11. Konsultierte juristische und technische Quellen
```

A.4 Aufzeichnung etwaiger Simulationen

Mindestdokumentation

```
Frage und Kennzahl: [was verglichen wird]
Einbezogene Daten und Abdeckung: [Quelle und Filter]
Gewählte Referenz und Begründung: [Zeitraum oder Gruppe]
Permutationsregeln: [was erhalten bleibt und was sich ändert]
Seed und Werkzeugversion: [für die Wiederholung]
Iterationen: [Anzahl und Begründung]
Ergebnis: [Verteilung und Beobachtung]
Nicht abgebildete Voraussetzungen: [Einschränkungen]
Zulässige Schlussfolgerung: [ohne fiktive Wahrscheinlichkeit]
```

Anhang B. Rechtsrahmen und Abschlusskontrolle

Das Beweismaterial aus Beiträgen und Protokollen wird mit der Anerkennung, Aufbewahrung und Bewertung elektronischer Dokumente verbunden. Mexiko verwendet CCom 89–94 und 1205 sowie CFPC/CNPCF entsprechend dem Übergangsregime; Peru trennt Signatur und Verfahren; Chile unterscheidet Signaturarten und Datum; Argentinien bewertet die Zuverlässigkeit; Kolumbien und Ecuador verlangen Aufbewahrung mit Herkunft und Datum; Spanien verbindet eIDAS, LEC und digitale

Dienste. Spontane Inhalte werden nicht ohne Prüfung des jeweiligen Regimes mit Werbung gleichgesetzt.[3456789101112131415]

Die Untersuchung von Netzwerken betrifft ebenfalls personenbezogene Daten. Zweckbindung, Verhältnismäßigkeit, Sicherheit und Datenminimierung sind anzuwenden; Quellen werden nicht ohne Grundlage kombiniert, um eine Person zu identifizieren. Meinungsfreiheit und Inhaltsanalyse werden getrennt von der Bewertung koordinierten Verhaltens behandelt. Die Bezeichnung als „Bot“ kann falsch und schädlich sein, auch wenn ein Konto ein Pseudonym verwendet.[15161718]

Abschlusskontrolle	Prüffrage
Abdeckung	Sind Abfrage, Filter, Zeitraum und fehlende Daten dokumentiert?
Objekte	Hat jeder Beitrag, jede Beziehung und jede Kennzahl eine Quelle?
Koordination	Liegen konvergierende Indizien und ein Referenzvergleich vor, nicht nur eine Koinzidenz?
Alternativen	Wurden Vorlage, Ereignis, Community und Plattform bewertet?
Graph	Wird weder ein Knoten mit einer Person noch eine Kante mit Kontrolle gleichgesetzt?
Attribuierung	Nennt die Schlussfolgerung keine unbelegten Inhaber oder Werkzeuge?
Schaden	Sind Reichweite und Folgen getrennt und belegt?
Datenschutz	Vermeidet die Untersuchung unnötige Offenlegung?

Abschluss

Das Netzwerk wird anhand von Objekten, Abfolge und Beziehungen nachgewiesen. Eine Person wird nicht erfunden, um die Grafik zu vervollständigen.

[3] Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Offizielle Textfassung. Offizielle Online-Quelle

[4] Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Textfassung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von den entsprechenden förmlichen Erklärungen ab. Offizielle Online-Quelle

[5] Peru. Reglamento de la IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung und Zulassung elektronischer Dokumente mit digitaler Signatur. Offizielle Online-Quelle

[6] Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Beweismittel, Beweislast, Beweiswürdigung und Datumsangaben durch technische Mittel. Offizielle Online-Quelle

[7] Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert. Offizielle Online-Quelle

[8] Argentinien. Código Civil y Comercial, Artikel 318–319: Korrespondenz mit beliebigen Mitteln und Würdigung der Zuverlässigkeit von Datenträgern und technischen Verfahren. Offizielle Online-Quelle

[9] Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur. Offizielle Online-Quelle

[10] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur. Offizielle Online-Quelle

[11] Verordnung (EU) 910/2014 eIDAS, Artikel 25–26 und 46: Nichtdiskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene Signatur und Rechtswirkungen qualifizierter Signaturen. Offizielle Online-Quelle

[12] Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Werkzeuge zum Speichern, Abrufen oder Reproduzieren von Daten, Prüfung, Verwahrung und vernünftige Beweiswürdigung. Offizielle Online-Quelle

[13] Verordnung (EU) 2022/2065 über digitale Dienste. Regelungen für Vermittlungsdienste, Management systemischer Risiken bei bestimmten sehr großen Plattformen und Suchmaschinen sowie Inhaltsregeln. Sie macht nicht aus jedem Muster einen Beweis für Koordination oder aus jeder Meinung rechtswidrige Inhalte. Offizielle Online-Quelle

[14] Verordnung (EU) 2024/900 über Transparenz und Targeting politischer Werbung. Besondere Regeln für politische Werbedienste und damit verbundene Risiken; sie gilt nicht undifferenziert für alle spontanen Inhalte von Nutzern. Offizielle Online-Quelle

[15] Mexiko. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Text veröffentlicht am 20-03-2025 und Reform vom 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Sicherheitsverletzungen und Wahrnehmung von Rechten. Die derzeitige Bundesbehörde ist die Secretaría Anticorrupción y Buen Gobierno. Offizielle Online-Quelle

[16] Kolumbien. Ley Estatutaria 1581 de 2012, Artikel 4, 8, 12, 17–18 und 26: Grundsätze, Rechte, Information, Pflichten von Verantwortlichen und Auftragsverarbeitern sowie Übermittlung in Drittländer. Offizielle Online-Quelle

[17] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Technikgestaltung, Risiken und Vorgehen bei Vorfällen. Offizielle Online-Quelle

[18] Europäische Union. Verordnung (EU) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit sowie Meldung und Benachrichtigung bei Sicherheitsverletzungen. Für Spanien ist zusätzlich das anwendbare nationale und sektorielle Recht zu prüfen. Offizielle Online-Quelle