Handreichung für Betroffene

Was tun bei ausländischer Informations-manipulation?

Erkennung, Sofortmaßnahmen und nachhaltige Absicherung

Bundesministerium des Innern

Manipulierte Bilder von angeblichen Fehltritten, vermeintlich „authentische“ Telefonmitschnitte mit skandalösen Aussagen oder eine täuschend echt nachgebaute Seite eines Nachrichtenmagazins – all das können Erscheinungsformen von Informationsmanipulation durch staatsnahe ausländische Akteure sein. Diese Handreichung soll potenziell Betroffenen helfen, von staatsnahen ausländischen Akteuren gesteuerte Informationsmanipulation zu erkennen und gibt konkrete Handlungsempfehlungen.

Informationsmanipulation umfasst eine Vielzahl zielgerichtet eingesetzter Mittel. Darunter fällt z. B. eine unauthentische Reichweitenverstärkung, etwa durch automatisierte oder koordinierte Verbreitung von Inhalten, die Veränderung von Ton- und Bildmaterial oder die Verschleierung des staatlichen Urhebers. Ihr Ziel ist es, die verbreitete Botschaft künstlich zu verstärken bzw. das Urteilsvermögen der Zielgruppe zu untergraben.

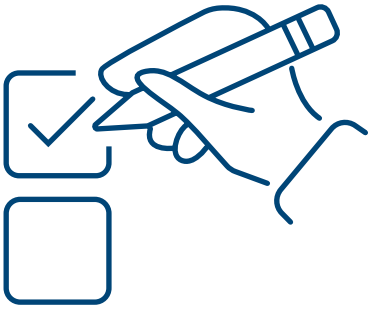


Wichtig ist dabei: **Nicht jede Informationsmanipulation ist auf einen ausländischen Staat zurückzuführen.** Urheberschaft (staatlich oder privat, In- oder Ausland) und Motivation (politisch, finanziell) von Akteuren im Bereich der Informationsmanipulation sind nicht sofort erkennbar.

Die folgende **Checkliste** soll Ihnen helfen, **Verdachtsfälle** zu erkennen. Die aufgeführten Verdachtsmomente reichen für sich genommen nicht aus, eine Aktivität eines ausländischen staatsnahen Akteurs nachzuweisen oder belastbare Aussagen über den Urheber zu treffen. Sie können z. T. auch Belastungsindikatoren in anderen Sachzusammenhängen sein (siehe z. B. Doxing). Da sich Informationsmanipulation mit anderen Phänomenbereichen überschneiden kann und Inhalte gezielt manipuliert werden, besteht das Risiko einer falschen Zuschreibung. Eine solche Fehleinschätzung kann bei einer Veröffentlichung der Reputation von Betroffenen schaden.

Sind Sie möglicherweise von Informationsmanipulation durch einen staatlichen oder staatlich gelenkten ausländischen Akteur betroffen? Ziehen Sie keine voreiligen Schlüsse! Wenden Sie sich im Zweifelsfall an die Projektgruppe Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (Infomanipulation@bmi.bund.de). Dort erhalten Sie eine erste Einschätzung des Vorfalls. Bei Bedarf werden Sie an weitere zuständige Stellen verwiesen und zu den nächsten Schritten beraten.

1 Checkliste



Bin ich von Informationsmanipulation durch staatsnahe ausländische Akteure betroffen?

Mögliche Anzeichen

- ☐ Plötzlicher, sprunghafter Anstieg von Erwähnungen der betroffenen Person oder einzelner Aussagen in sozialen Medien ohne erkennbaren Anlass.
- ☐ Private, nicht-öffentliche Informationen wie die Privatadresse oder die Telefonnummer oder Familiendetails wurden veröffentlicht (Doxing).

> **Doxing:** Die gezielte Veröffentlichung privater, z. T. nicht-öffentlicher Informationen einer Person im Internet – oft zur Einschüchterung oder um koordinierte Belästigung zu ermöglichen.

- ☐ Die verbreitete Botschaft über die betroffene Person steht im Einklang mit einem ausländischen staatlichen Narrativ bzw. dem strategischen Interesse eines ausländischen Staates.
- ☐ Andere Betroffene sind zeitgleich Ziel von vergleichbaren, koordinierten Aktivitäten.
- ☐ Viele Accounts posten nahezu zeitgleich sehr ähnliche Formulierungen oder identische Inhalte.
- ☐ Die Verbreitung geschieht über mehrere Plattformen hinweg.

> **Beteiligte Accounts zeigen Bot-Merkmale:** sie sind kürzlich erstellt, haben generische Profilbilder oder weisen ungewöhnliche Interaktionsmuster auf, wie z. B. synchronisierte oder gleichlautende Kommentarwellen, kurzfristig wiederkehrende und wechselseitige Likes und Reposts.

- ☐ Manipulierte Informationen erscheinen zuerst auf ausländischen Plattformen und werden dann in den deutschen Informationsraum übertragen.
- ☐ Manipulierte Informationen werden von erkennbar staatsnahen ausländischen Kanälen veröffentlicht oder weiterverbreitet.
- ☐ Deepfakes (aufwändig gefälschte Ton-, Bild- oder Videodateien) mit Konterfei oder andere Formen der Imitation der Identität (z. B. Fake-Profile, gefälschte Zitate) werden in Umlauf gebracht.
- ☐ Manipulierte Informationen werden im zeitlichen Zusammenhang zu politischen Anlässen (z. B. Wahlen, Gipfeltreffen, politischen Entscheidungen) in Umlauf gebracht.

Bots/Bot-Netzwerke: Automatisierte Accounts, die massenhaft Inhalte verbreiten, um künstlich Reichweite zu erzeugen.

Treffen mehrere Anzeichen zu, kann dies auf einen Versuch ausländischer Informationsmanipulation hindeuten. Wenden Sie sich auch hierfür gerne an die o. g. E-Mail-Adresse.

Maßnahmen: Was tun, wenn ich den Verdacht habe, von Informationsmanipulation durch staatsnahe ausländische Akteure betroffen zu sein?

Von Informationsmanipulation betroffen zu sein, kann beängstigend und persönlich herausfordernd sein. Achten Sie auf sich. Suchen Sie sich Hilfe und Beratung.

Vermeiden Sie vorschnelles Handeln. Treffen **wenige bis gar keine der genannten Anzeichen** auf den Vorfall zu, könnte eine unmittelbare öffentliche Reaktion bzw. Kommunikation das Gegenteil von dem bewirken, was Sie erreichen wollen: Anstatt zur Aufklärung beizutragen, kann Ihre Reaktion die Aufmerksamkeit erst auf die ursprüngliche Manipulation lenken (Streisand-Effekt).

Wenn auf den Vorfall **mehrere Anzeichen** zutreffen, ist zeitnahes Handeln empfehlenswert. Gleichzeitig können auch einzelne, sehr schwerwiegende Indikatoren (z. B. Doxing) sofortiges Handeln erfordern. Mehr dazu im folgenden Abschnitt.

2 Sofortmaßnahmen

Wie reagieren, wenn eine Reaktion innerhalb der ersten 24 bis 48 Stunden erforderlich ist?

Grundregel: Nicht öffentlich reagieren, bevor Sie die Lage eingeschätzt und Ihre Reaktion sorgsam geplant haben.

Denn: Schnelle und unkoordinierte öffentliche Reaktionen können den verbreiteten Botschaften zusätzliche Reichweite verschaffen und bei Fehleinschätzungen zu Reputationsschäden führen.

Schritt 1:
Wenn nötig, Strafverfolgungsbehörden informieren

Wenn Sie eine strafrechtliche Relevanz oder eine durch den Vorfall der Informationsmanipulation hervorgerufene Bedrohungssituation vermuten, binden Sie die zuständige Polizeidienststelle möglichst frühzeitig ein und folgen Sie den Anweisungen der Strafverfolgungsbehörden.

Schritt 2:
Lage dokumentieren

Sichern Sie mithilfe von Screenshots, Links, Zeitstempel etc. alle relevanten Inhalte zum Sachverhalt. Dokumentieren Sie den Sachverhalt zunächst inhaltlich. Orientieren Sie sich bei der weiteren Dokumentation an den o. g. Anzeichen, die Ihren Anfangsverdacht begründen.

Schritt 3:
Intern koordinieren

Informieren Sie ggf. umgehend Kollegen, Ihr Team oder Ihre Organisation. Benennen Sie eine verantwortliche Person für die weitere Koordination der Reaktion und die Beobachtung der weiteren Verbreitung der Inhalte. Stellen Sie sicher, dass niemand zu dem Vorfall unabgesprochen öffentlich kommuniziert und hierdurch ggf. die verbreitete Botschaft ungewollt verstärkt wird.

Schritt 4:
IT-Sicherheit verstärken

Aktivieren Sie sichere Zugangsmethoden zu Ihren Profilen wie z. B. die Zwei-Faktor-Authentifizierung auf allen Plattformen und ändern Sie Ihre Passwörter. Prüfen Sie aktive Zugriffe auf Ihre Konten in Netzwerken und entfernen Sie unbekannte Geräte. Bei koordinierten Angriffen kann unter besonders dringlichen Umständen z. B. die Kommentarfunktion vorübergehend eingeschränkt werden. Weitere Hinweise finden Sie beim Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html).



Schritt 5:
Relevante Stellen und Personen kontaktieren

Informieren Sie ggf. die für Informationssicherheit zuständigen Stellen und Personen in Ihrer Organisation.

Leiten Sie eine Überprüfung von Inhalten und Verhaltensweisen bzw. eine Löschung durch den Plattformbetreiber erst nach der (ggf. polizeilich-forensischen) Sicherung relevanter Daten ein. Die Gemeinschaftsrichtlinien der Social-Media-Anbieter enthalten eigene Regeln zum Umgang mit Informationsmanipulation (z. B. zum Thema Fake-Accounts). Sie sind nach dem Digital Services Act (DSA) verpflichtet, diese durchzusetzen. Kommen sie dem wiederholt nicht nach, kann dies über das Beschwerdeportal (https://www.dsc.bund.de/DSC/DE/3Verbraucher/start.html) beim Digital Services Coordinator (DSC) gemeldet werden.



Schritt 6:
Kommunikation abstimmen

Entscheiden Sie gemeinsam mit Ihrem Team bzw. Ihrer Organisation, ob und wie Sie öffentlich reagieren:

Wenn eine öffentliche Reaktion zum aktuellen Zeitpunkt voraussichtlich eher negative Folgen hätte – etwa zusätzliche Reichweite für die verbreitete Botschaft –, sollten Sie die Entwicklung dennoch regelmäßig beobachten und neu bewerten.

Sollten Sie sich für eine Reaktion entscheiden, benennen Sie bei einer öffentlichen Kommunikation die Fakten und ordnen Sie die zu widerlegende Botschaft ein, ohne diese wörtlich zu wiederholen. Geben Sie dabei detaillierte Gegenargumente und erläutern Sie eindeutig, warum die fragliche Information oder Meldung nicht zutrifft.

Neben der Widerlegung falscher Darstellungen ist es auch wichtig, die Manipulationsmethoden und irreführenden Argumentationsmuster zu benennen und zu erklären. Dies trägt dazu bei, die Widerstandsfähigkeit gegenüber zukünftigen Manipulationsversuchen zu erhöhen. Bereiten Sie einordnende und kontextualisierende Informationen für Medienanfragen vor.



Schritt 7:
Monitoring aufsetzen

Richten Sie in Ihrem Team ein (temporäres) Social-Media-Monitoring ein. Beobachten Sie, ob die koordinierten Aktivitäten ausländischer Einflussnahme abnehmen oder noch weiter zunehmen.

3 Mittel- und langfristige Maßnahmen

Was tun, wenn die erste Welle vorbei ist?

Grundregel: Wenn die Akutphase überstanden ist, gilt es, die richtigen Weichen für eine nachhaltige Absicherung zu stellen.

Die folgenden Maßnahmen sollten innerhalb der ersten Wochen nach dem Vorfall angegangen werden.



Schritt 1:
Vorfall systematisch dokumentieren

Erstellen Sie gemeinsam mit Ihrem Team eine strukturierte Dokumentation des Vorfalls im Zeitverlauf: Stellen Sie anhand eines Zeitstrahls die Verbreitungswege, die beteiligten Plattformen und Netzwerke, die Reichweite, ggf. identifizierte Akteure und die Rezeption in den Medien dar. Diese Dokumentation dient als Grundlage für Ihre persönliche Prävention, ggf. weitere Schritte und sichert Ihre Erkenntnisse für die Zukunft.



Schritt 2:
Für die Zukunft lernen

Besprechen Sie mit Ihrem Team und Ihrer Organisation, was gut funktioniert hat und wo Verbesserungsbedarf besteht im Hinblick auf die Reaktionsgeschwindigkeit, interne Kommunikationswege, Zuständigkeiten etc. Halten Sie die Ergebnisse schriftlich fest.

Entwickeln Sie einen Notfallplan für zukünftige Vorfälle oder passen Sie bestehende Pläne an: Wer entscheidet über eine öffentliche Reaktion? Wer koordiniert intern? Soll evtl. ein professioneller Dienstleister zur Unterstützung hinzugezogen werden? Welche Informationen und Vorlagen liegen für eine Reaktion bereit? Auf welchen Kanälen kommunizieren Sie im Notfall, und in welcher Form? Wer kann Sie bei Ihrer Reaktion unterstützen (Kontakte zu Medien etc.)?



Schritt 3:
Digitale Resilienz stärken

Führen Sie ein IT-Sicherheits-Audit für alle Geräte und Ihre Accounts durch (sowohl berufliche als auch private). Schulen Sie Ihr Team zu Methoden und Merkmalen ausländischer Einflussnahme und Informationsmanipulation. Richten Sie ggf. ein dauerhaftes Basis-Monitoring für Ihre Online-Präsenz ein.

Impressum

Herausgeber
Bundesministerium des Innern, 11014 Berlin
Internet: www.bmi.bund.de

Gestaltung
familie redlich AG – Agentur für Marken und Kommunikation
P.E.R. Agency GmbH

Bildrechte
S. 2: Father_Studio / stock.adobe.com

Stand
August 2026

Artikelnummer
BMI26007

Weitere Publikationen der Bundesregierung zum
Herunterladen und zum Bestellen finden Sie unter:
www.publikationen-bundesregierung.de

Diese Publikation wird von der Bundesregierung im Rahmen ihrer Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.

www.bmi.bund.de
bsky.app/profile/bmi.bund.de
instagram.com/bmi_bund
linkedin.com/company/bundesinnenministerium
social.bund.de/@bmi
threads.com/@bmi_bund
x.com/BMI_Bund
www.youtube.com/@BMIBund