Neue Zürcher Zeitung

Deepfake, Propaganda oder Augenzeugenbericht von der Front: Wie man als normaler Nutzer im Informationskrieg nicht den Überblick verliert

Der Krieg in der Ukraine beschert uns auf Tiktok, Twitter und Facebook eine Flut von Beiträgen: Manche sind echt, manche irreführend, manche falsch. Eine Anleitung zum Umgang damit in sieben Schritten.

Philipp Gollmer

19.03.2022, 05.35 Uhr

Reuters

Ausschnitte aus einem auf Social Media geteilten Video, das einen Raketenangriff auf ein Regierungsgebäude in Charkiw am 1. März 2022 zeigt.

Jede Person hat heute die Möglichkeit, den Krieg in der Ukraine quasi in Echtzeit online mitzuverfolgen – oder zumindest ein bestimmtes Abbild davon. Wer sich auf Social Media oder Nachrichtendienste wie Telegram begibt, wird mit einer Flut von Beiträgen konfrontiert. Diese können wahr oder falsch, aus dem Kontext gerissen oder regelrechte Propaganda sein. In dem Strudel von Bildern, Videos, Nachrichten und Meinungen ist es schwer einzuschätzen, welchen Informationen man vertrauen kann.

Am Mittwoch tauchte zum Beispiel ein gefälschtes Deepfake-Video von Wolodimir Selenski auf. Darin fordert der ukrainische Präsident scheinbar seine Truppen auf, die Waffen niederzulegen. Das Video war leicht als Fälschung zu erkennen: In der Aufnahme hat Selenski einen seltsam grossen Kopf, der unschärfer ist als der Rest seines Körpers, und seine Stimme ist tiefer als üblich. Das Video wurde inzwischen von den Meta-Plattformen entfernt.

Selbst die Profis stossen derzeit an Grenzen, wenn es darum geht, Bilder und Videos aus dem Kriegsgebiet zu verifizieren. Forrest Rogers, Osint-Reporter (open source intelligence) bei der NZZ, sagt: «Zu Beginn des Krieges konnte man Informationen zuverlässig überprüfen. Gegenwärtig ist es jedoch extrem schwierig, den Wahrheitsgehalt eines Videos auf Social Media zu bestimmen.» Oft lasse sich zwar noch der Ort der Aufnahme verifizieren, nicht aber eine genaue Uhrzeit oder ein Datum.

Auch wenn die Lage zunehmend unübersichtlich wird: Wer gewisse Punkte beachtet, behält auch während einer sich rasch verändernden Nachrichtenlage den Überblick.

Inhaltsverzeichnis

Durchatmen ↑

Soziale Netzwerke sind darauf ausgelegt, dass Inhalte schnell weiter geteilt werden. Doch egal wie traurig, wütend oder glücklich ein bestimmter Beitrag einen macht und egal wie gross das Bedürfnis ist, ihn mit seinem Netzwerk zu teilen, man sollte kurz innehalten und einmal tief durchatmen.

Gerade in einer unübersichtlichen Situation wie dem Krieg in der Ukraine sollte man sich erst genauer mit Inhalt, Absender und Quelle eines Beitrags beschäftigen und immer von der Möglichkeit ausgehen, dass die auf Social Media geteilten Beiträge, Fotos und Videos falsch sind. «Wenn es zu abgedreht klingt, um wahr zu sein, ist es das wahrscheinlich auch nicht», sagt Rogers.

Wer ist der Absender?

In einem ersten Schritt sollte man einen Blick auf das Profil des Absenders werfen. Wie lange existiert der Account bereits, und wie viele Follower hat das Profil? Bei sehr jungen Accounts oder solchen mit wenigen Followern ist Vorsicht geboten.

Auch die bisher veröffentlichten Beiträge sollten überprüft werden. Sie können einen Hinweis über die Interessen und Überzeugungen des Absenders liefern. Haben sich der Ton und die Art der Beiträge jüngst verändert, könnte das ein Hinweis auf einen gehackten Account sein. Ein blauer Verifizierungshaken oder eine private Verbindung machen das Profil oder den Inhalt der Nachricht nicht automatisch vertrauenswürdig.

Hat das Profil eine Verbindung zu einer Website, lohnt sich ein Blick ins Impressum. Wenn es fehlt, ist das ein schlechtes Zeichen. Verweisen die Angaben darin auf Personen oder Firmen, kann eine Google-Suche helfen, mehr über den oder die Urheber herauszufinden.

Handelt es sich um eine seriöse Quelle?

Weitere Hinweise darauf, ob ein Beitrag vertrauenswürdig ist, kann ein Blick auf die Quelle der Information liefern. Stammt sie vom Urheber selber, der möglicherweise vor Ort ist oder ein Experte auf dem Gebiet? Oder verweist der Beitrag auf eine Organisation, eine Zeitung oder eine Behörde? Hier kann eine Google-Suche helfen, um die Seriosität einer

Quelle zu überprüfen. Das Fehlen einer Quelle ist ein Alarmsignal.

Vorsicht ist auch bei Screenshots von Informationen oder Aussagen geboten. Diese könnten aus dem Zusammenhang gerissen sein und ein falsches Bild der Sachlage vermitteln. Eine umgekehrte Bildsuche (siehe unten) oder eine Suche nach dem genauen Wortlaut können hier allenfalls helfen, mehr Kontext zum Beitrag zu finden.

Wie ist der Beitrag aufbereitet? ↑

Falschnachrichten sind oft stark emotionalisiert. Reisserische Texte und aufwühlende Bilder sollen beim Nutzer starke Gefühle auslösen und ihn damit zum Kommentieren und Teilen verleiten. Auch Rechtschreibfehler oder ein chaotisches Layout können ein Hinweis auf einen unseriösen Inhalt sein.

Weitere Informationen einholen ↑

Enthält ein Beitrag keine Hinweise auf eine Quelle, lohnt sich ein Blick auf vertrauenswürdige Nachrichten-Websites oder Experten. Diese stützen sich im Idealfall auf unterschiedliche Quellen und können helfen, die auf Social Media entdeckte Information einzuordnen. Fehlen Medienberichte zum Thema oder lassen sich gar keine weiteren Hinweise dazu auftreiben, ist Vorsicht geboten.

Neben klassischen Nachrichtenportalen bieten auch die Portale von

Faktencheckern eine Orientierungshilfe, etwa jene von DPA, AFP oder Reuters. Auch die Social-Media-Plattformen selbst können Beiträge, die Falschinformationen enthalten, mit einem entsprechenden Hinweis versehen oder entfernen – allerdings tun sie das oft nur mit Verspätung. Neuerdings werden auch Accounts mit Verbindungen zu staatlichen Akteuren von den Plattformen transparenter markiert.

Bilder und Videos überprüfen

Besonders bei Fotos und Bewegtbildern ist Vorsicht geboten. Wurde die Aufnahme tatsächlich am angegebenen Ort und zur angegebenen Zeit gemacht? Bei Fotos kann Klarheit schaffen, das Bild im Netz nachzuschlagen, um herauszufinden, ob es schon an anderer Stelle verwendet wurde. So eine Bilder-Rückwärtssuche gibt es zum Beispiel bei Google. So wird schnell klar, wann die Aufnahme gemacht wurde und in welchem Kontext.

Falsche Videos zu entlarven, ist für Laien hingegen etwas schwieriger. Mit einem klaren Screenshot aus dem Video lässt sich durch eine Bildersuche allenfalls das Original finden. Es gibt weiter Dienste, die dabei helfen, herauszufinden, wie alt ein Video tatsächlich ist und ob es zuvor schon an anderer Stelle einmal hochgeladen wurde. Für Youtube zum Beispiel der Dataviewer von Amnesty International.

Ukraine: Wie man False-Flag Videos erkennt

Wie erkennt man False-Flag Videos?

NZZ Video

Gelingt es der NZZ, die Echtheit eines Videos zum Krieg in der Ukraine zu bestätigen, wird das mit dem Hinweis «Dieses Video wurde von der NZZ verifiziert» gekennzeichnet. Das signalisiert den Leserinnen und Lesern, dass strenge Kontrollen durchlaufen worden sind, um die Richtigkeit sicherzustellen.

Deepfakes erkennen

Eine weitere Art, wie in Video- und Audioform Falschinformationen verbreitet werden können, sind Deepfakes. Dabei wird mithilfe von künstlicher Intelligenz und maschinellem Lernen das Gesicht oder die Stimme einer Person manipuliert, um ihr eine erfundene Aussage in den Mund zu legen oder sie in einem ungünstigen Kontext erscheinen zu lassen.

Um ein Deepfake zu entlarven, kann man auf einige Punkte achten.

Zunächst einmal gilt es auch hier, innezuhalten und kurz zu überlegen: Ergibt das gerade Gesehene oder Gehörte tatsächlich Sinn? Zudem sollte man den Inhalt über eine andere, vertrauenswürdige Quelle überprüfen.

Weiter kann man in der Aufnahme nach Unstimmigkeiten suchen. Seltsame Sprünge im Video, schlechte Lippen-Synchronisation, eine veränderte Stimmlage, verschwommene Stellen oder ungewöhnliche Schattenwürfe sowie komisch aussehende Gliedmassen sind alles Hinweise auf ein Deepfake. Auch ein perfekt symmetrisches Gesicht oder eine verformte Brille sind typische Merkmale eines solchen Videos. Gerade Haare, Ohren und andere feine Details wie Schmuck und Zähne sind sehr schwer zu manipulieren. Bei der Überprüfung kann es helfen, sich das Video verlangsamt oder Bild für Bild anzusehen.

Passend zum Artikel

Das bombardierte Kinderspital in Mariupol im Strudel des Informationskriegs

11.03.2022

KOMMENTAR

Informationskrieg um die Ukraine: warum es jetzt so wichtig ist, dass unabhängige Medien mit neuster Technik nach Russland schauen

16.02.2022

Im Ringen gegen Fake News könnte eine «Impfung» wirksamer sein als jeder Faktencheck

15.02.2022

Das FBI warnt vor Deepfakes, Facebook behauptet, es habe eine Lösung – entstanden sind sie als Kollateralschaden einer klugen Idee

10.07.2021

Mehr zum Thema Ukraine

Alle Artikel zum Thema >

Waffen an die Ukraine: Was Deutschland tut – und was nicht

13.04.2022

Ein General mit Syrien-Erfahrung soll Russland in der Ukraine zum Sieg führen – wird ihm das gelingen?

13.04.2022

Ukrainische Flüchtlinge kehren zurück in die Heimat: «Wir hoffen auf das Beste, aber erwarten das Schlimmste»

13.04.2022

Weitere Themen Social Media

Für Sie empfohlen

Weitere Artikel >

SERIE

Kriegstagebuch aus Charkiw (36): Der Putinophile im Zoo

13.04.2022

Mehr Sicherheit, mehr Sanktionen, mehr Solidarität – mehr Stimmen? Burkart und Pfister wollen ihre Parteien wieder staatstragend machen

vor 3 Stunden

Pierin Vincenz: wie er wurde, was er ist

vor 3 Stunden

Bis die Gitarre wimmert und schluchzt – Johnny Winter ist eine Legende aus der grossen Zeit der Rock-Solisten. Nun lebt sein Blues wieder auf

13.04.2022

Sollen Russlands Schachmeister ausgeschlossen werden? Da gibt es kein Schwarz oder Weiss wie auf dem Brett

13.04.2022