BILD GINA SANDERS – FOTOLIA; ILLUSTRATION: STELLER / QUELLEN: UNIVERSITY OF SOUTHERN CALIFORNIA, STANFORD UNIVERSITY

Fälschungen erkennen

Skepsis: „Der erste Schritt beim Erkennen von sogenannten Fake News (falsche Nachrichten) ist ein gewisses Gefühl“, sagt Andre Wolf von Mimikama, einer Koordinationsstelle zur Bekämpfung von Internetmissbrauch. Überspitzte Darstellung und das Fehlen belastbarer Quellen können Anzeichen sein. Hier ist also Misstrauen gefragt. Gerade das fehlt vielen Internetnutzern aber: Eine Studie der US-Universität Stanford etwa kam zu dem Ergebnis, dass gerade junge Menschen einfach hinters Licht geführt werden können.

Impressum: Wer sich unsicher ist, ob die Nachricht der Wahrheit entspricht, sollte die Quelle anschauen. Das bedeutet auch: In sozialen Netzwerken erst prüfen, woher etwas kommt – und es dann teilen. Auf der Ursprungsseite lohnt dann vor allem der Blick ins Impressum. „Wenn es gar keins gibt, sollte man aufmerksam werden“, rät der Experte.

Suchmaschine: Das Gegenchecken von Texten und Bildern kann helfen, falsche Nachrichten zu erkennen. Wenn Google und Co. Textstellen auf mehreren Webseiten abseits seriöser Nachrichtenportale wiederfinden, ist das ein Indiz für Fake News. „Viele alternative Blogs nehmen Inhalte und kopieren sie einfach unreflektiert“, sagt Wolf. Bei Fotos kann die Bildersuche helfen. Ist ein angeblich aktuelles Foto beispielsweise schon 2008 im Netz aufgetaucht, kann irgendwas nicht stimmen.

Melden: Bei Mimikama können Internetnutzer Fake News melden. Die Initiative prüft die Nachricht und verfasst dann eventuell einen Bericht darüber. Die Initiative betreibt unter **www.hoaxsearch.com** außerdem eine Suchmaschine für Fake News. (dpa)

Der netzpolitische Sprecher der SPD-Bundestagsfraktion, Lars Klingbeil, wundert sich indes darüber, dass sich „Facebook nicht längst in die Expertise von Journalisten und Wissenschaftlern investiert, um offensichtlich Fakes aufzudecken und einzuordnen“, hieß es laut Medienberichten. Dies scheint sich jedoch zu ändern. „Business Insider“ berichtete, dass Facebook gerade an einem neuen Angebot feilt. Dabei sollen von seriösen Medien kuratierte Nachrichten in die Facebook-Ansicht integriert werden. Das Projekt befinde sich noch in der Testphase.

Doch nicht nur falsche Nachrichten in sozialen Netzwerken bereiten vielen Sorge – Politiker und Netzexperten fürchten auch Manipulationen der Bevölkerung durch sogenannte Social Bots. Diese programmierten Software-Roboter „sammeln Informationen und Daten und haben die Aufgabe, die Meinung in sozialen Netzwerken zu beeinflussen, ohne dass der Nutzer dies bemerkt“, erklärt der Konstanzer Informatik-Professor Jürgen Neuschwander. Während des US-Wahlkampfes in den USA sollen Hunderttausende solcher Roboter im Einsatz gewesen sein. Forscher der University of Southern California in Los Angeles sprechen zum Beispiel davon, dass etwa 20 Prozent der Twitter-Follower von Hillary und Trump keine echten Menschen, sondern Maschinen waren.

Sachsen-Anhalts Kulturminister Rainer Robra (CDU) forderte deshalb ein Verbot sogenannter Social Bots. Zielen soll es auf Programme, die automatisiert in eine Richtung kommentieren, dabei aber den Eindruck erwecken, es handele sich um eine echte Person hinter dem Profil – oftmals versehen mit Namen und Foto. Rechtsexperte Moritz Hennemann hält jedoch dagegen: „Ein pauschales Verbot aller Einsatzmöglichkeiten von Social Bots dürfte wohl nicht zielführend und auch sehr schwierig durchzusetzen sein“, meint er und gibt zu bedenken, dass die Roboter in vielfältigen Konstellationen eingesetzt werden – „positiv wie negativ“.

Doch wie viel Macht haben solche Maschinen tatsächlich? Das Beeinflussungspotenzial von Bots lässt sich nur schwer vorhersagen, erklärt Neuschwander. „Es gibt dazu noch keine wissenschaftlich belastbaren Untersuchungen“. Außerdem sei es schwer bis unmöglich die Maschinen von Menschen zu unterscheiden, zumal diese „durch den Einsatz neuer Technologien aus der künstlichen Intelligenz qualitativ immer besser werden“. Die im Bundestag vertretenen politischen Parteien haben die Brisanz des Themas erkannt und wollen von Social Bots im Wahlkampf keinen Gebrauch machen, sagte der CDU-Politiker Rainer Robra.

Ein weiteres Mittel zur Manipulation vor einer Wahl sind offenbar Cyberattacken. So verdichten sich die Hinweise, dass Russland in den US-Wahlkampf eingegriffen haben könnte. Geheimdienste sind nach einem Medienbericht davon überzeugt, dass der russische Präsident Putin Anweisungen im Zusammenhang mit den Hackerangriffen auf die Demokraten gegeben hat, zunächst aus Rache, dann um das politische System korrupt wirken zu lassen. Putins Sprecher Dmitri Peskow wies den Bericht zurück. Es handele sich um „lächerlichen Unsinn“.

Auch hierzulande fürchten Politiker Cyberangriffe. Deutschland muss sich nach Einschätzung von Angela Merkel (CDU) in Zukunft auf weitere Hacker-Attacken einstellen, sagte die Bundeskanzlerin nach dem gescheiterten Versuch von Hackern, knapp eine Million Router der Telekom zu kapern. Zu den Spekulationen, dass Russland auch hinter diesem Großangriff stecken könnte, sagte sie nichts. Laut Jürgen Neuschwander ist es schwer, zu beweisen, ob Russland hinter diesem und anderen Angriffen stecken könnte. Auch Hennemann kann die Vorwürfe nicht abschließend bewerten. „Die Technik des Internets bedingt es, dass nicht in jedem Fall konkret nachverfolgt werden kann, auf welche Weise und von wem eine Meldung verbreitet wird.“

Ob Cyberangriffe, falsche Nachrichten oder Maschinen auf Twitter: Letztlich hängt es auch von den Nutzern ab, wie sie die Informationen im Internet einschätzen, glaubt Hennemann. Jüngste Studien belegen, dass sich vor allem Jugendlichen schwer damit tun, seriöse Quellen zu erkennen. Neuschwander sieht deshalb nur einen Ausweg: eine verstärkte Medienkompetenz der Nutzer. Sie sollten sich fragen: Kann man die Quelle der Nachricht identifizieren? Gibt es andere Quellen und Medien, die dasselbe melden? Ist die Nachricht plausibel? Auch Hennemann sagt: „Es ist wichtig, entsprechende Medienkompetenzen und ein stärkeres Bewusstsein hierfür zu fördern.“

SK Kommunikationswissenschaftlerin Susann Kohout erklärt im Interview mit dem SÜDKURIER, warum im Internet gehetzt wird und wieso das Löschen von Kommentaren nicht unbedingt hilft. **www.sk.de/exklusiv**

Wird die Bundestagswahl manipuliert?

Berichte über eine mögliche Beeinflussung der US-Wahl durch russische Hacker und der Fall der Grünen-Politikerin Renate Künast alarmieren die deutsche Politik. Grund: Bald steht die Bundestagswahl an. Was ist an den Befürchtungen dran?

1 Teilen die Sicherheitsbehörden die Befürchtungen der Politiker? Ja. Der Cyber-Raum ist längst nicht mehr nur Schauplatz von „klassischer“ Kriminalität, sondern auch von Spionage, Sabotage, Manipulation und gezielter Desinformation. Das gilt insbesondere für die sozialen Medien. Das Bundesamt für Verfassungsschutz (BfV) wies zuletzt auf einen „eklatanten Anstieg“ sogenannter Spear-Phishing-Attacken gegen Parteien und Bundestagsfraktionen hin. Präsident Hans-Georg Maaßen warnte: „Die Hinweise auf Versuche einer Beeinflussung der Bundestagswahl im kommenden Jahr verdichten sich.“

2 Was wird damit bezweckt? Vor allem geht es darum, Unsicherheit zu schüren sowie das Vertrauen der Bürger in den Staat und seine Institutionen zu beschädigen. Ein Beispiel dafür war der Fall Lisa in Berlin. Im Internet hieß es, sie sei wohl von Migranten entführt und vergewaltigt worden. Beobachter sahen in dem Fall einen propagandaartigen Versuch der russischen Medien, in Russland und Deutschland Stimmung gegen Flüchtlinge zu machen.

3 Ist dies das einzige Ziel? Nein. Maaßen betonte, aus Cyberattacken erbeutete Informationen könnten im Wahlkampf auftauchen, um Politiker gezielt zu diskreditieren. Beispiel USA: Am Wochenende schrieben Medien über die Einschätzung des US-Geheimdienstes CIA, russische Hacker hätten mit hoher Wahrscheinlichkeit Computer der Demokraten angegriffen, um dem Republikaner Donald Trump zum Sieg bei der Präsidentenwahl über seine Rivalin Hillary Clinton zu verhelfen.

4 Ist Russland Haupt-Ausgangspunkt solcher Manöver? Wie reagiert Moskau auf solche Anschuldigungen? Der Verfassungsschutz hat seit dem Beginn der Ukraine-Krise einen erheblichen Anstieg russischer Propaganda- und Desinformationskampagnen in Deutschland registriert. Moskau bestreitet solche Aktionen – so auch die Vorwürfe aus den USA. Kremlsprecher Dmitri Peskow sprach von „unqualifizierten Behauptungen und Vorwürfen“, die mit der Realität nichts zu tun hätten. Die Regierungszeitung „Rossijskaja Gaseta“ warf amerikanischen wie deutschen Geheimdiensten Russophobie (Russlandfeindlichkeit) vor.

5 Gibt es in Russland Hinweise auf von dort gesteuerte Cyberangriffe? Naturgemäß äußert sich das Land nicht dazu. Ein Strategiepapier von Generalstabschef Waleri Gerassimow sieht aber vor, in den Kriegen der Zukunft Informationspolitik als Waffe zu verwenden. Bekannt sind die sogenannten „Trollfabriken“ in St. Petersburg. Deren Mitarbeiter überschwemmten nach dem russischen Vorgehen auf der Krim und in der Ostukraine 2014 soziale Netzwerke mit Kommentaren. Sie sollten das Vertrauen in die Berichterstattung westlicher Medien untergraben und die russische Sichtweise durchsetzen.

6 Lassen sich Urheber solcher Attacken im Internet nicht einfach ermitteln? Wenn es um Hackerangriffe geht, ist die Ermittlung der Täter in der Regel schwierig oder unmöglich. Das betonten zuletzt auch Internet-Experten anlässlich der Attacke auf ThyssenKrupp. Ermittler folgten Spuren – unter anderem nach China. Indiz dafür waren etwa die Angriffszeiten, die sich mit der dortigen Zeitzone deckten. Ein Beweis ist das aber nicht, es könnte auch eine falsch gelegte Fährte sein. Auch wenn die Standorte der Hauptserver ermittelt werden können, heißt das nicht, dass die Angriffe von dort ihren Ausgang nahmen. Auch sprachliche Fragmente in den Codezeilen, die auf eine Nationalität schließen lassen, können absichtlich eingefügt sein, um die Spur zu verwischen. Ob eine Attacke mit staatlicher Hilfe begangen wird, führen Ermittler meist auf deren Art zurück. Werden aufwendige Techniken verwendet, gilt dies meist als Beleg dafür, dass nicht allein Kriminelle dahinterstecken.

7 Wie sieht es bei sogenannten Fake-News aus? Es dürfte immer schwerer werden, die Echtheit von im Netz verbreiteten Nachrichten zu erkennen und schnell gegen Falschmeldungen vorzugehen – aktuelles Beispiel ist der Fall Künast. (dpa)