Die Schatten der Wahrheit: Desinformation als hybride Bedrohung

Von Holger Köster

Holger Köster

Geschäftsführer der HERSA-Unternehmensgruppe und Vorsitzender des Fachausschusses Wirtschaftsschutz im BDSW

In einer Welt, die zunehmend von digitalen Medien und globalen Informationsströmen geprägt ist, haben sich Desinformationskampagnen zu einem mächtigen Instrument politischer und strategischer Einflussnahme entwickelt. Besonders im Kontext hybrider Bedrohungen, also der gezielten Kombination verschiedener Mittel zur Destabilisierung von Staaten und Gesellschaften, spielen sie eine zentrale Rolle. Durch die Verbreitung manipulierter Informationen wird das Vertrauen in demokratische Institutionen, Medien und öffentliche Debatten untergraben. Der Einfluss von Desinformation reicht dabei von der Beeinflussung von Wahlen über die Verstärkung gesellschaftlicher Spaltungen bis hin zur Unterstützung geopolitischer Interessen autoritärer Akteure.

Der strategische Einsatz von Falschinformationen ist kein neues Phänomen, doch durch das Internet und insbesondere soziale Medien haben sich die Dynamiken verändert. Während klassische Propaganda oft von staatlich kontrollierten Medien ausging und klar als solche erkennbar war, sind moderne Desinformationskampagnen subtiler, vielseitiger und schwerer zu identifizieren. Akteure nutzen anonyme Plattformen, gefälschte Profile und KI-gestützte Technologien, um gezielt Unsicherheit zu säen und gesellschaftliche Meinungsbildungsprozesse zu beeinflussen. Diese Entwicklung stellt Demokratien vor erhebliche Herausforderungen, da sie nicht nur die Integrität politischer Systeme bedroht, sondern auch das gesellschaftliche Vertrauen in wissenschaftliche Erkenntnisse und objektive Berichterstattung erschüttert.

Ihr
Holger Köster

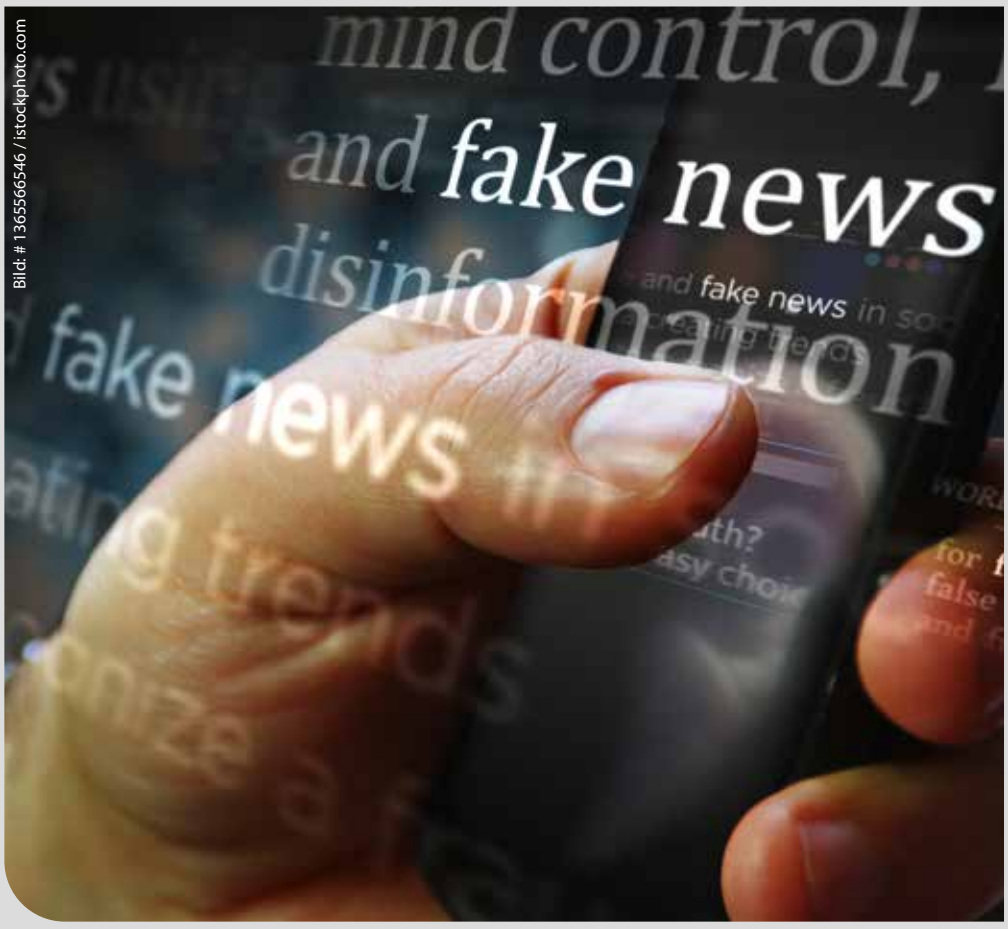


Bild: # 1365566546 / istockphoto.com

Desinformation als hybride Bedrohung

Von Holger Köster

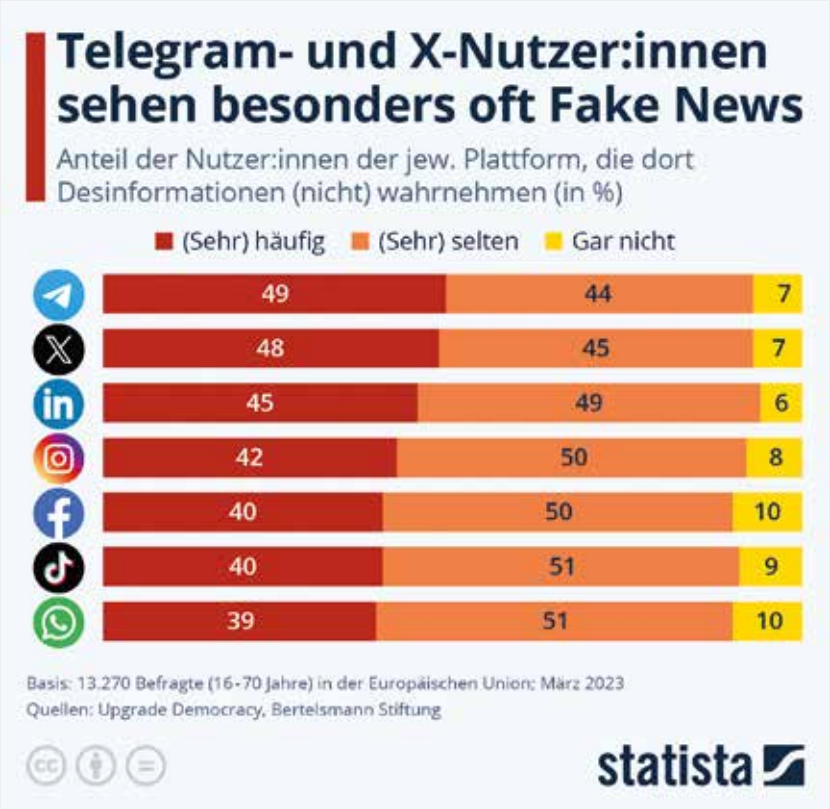
Desinformationskampagnen sind darauf ausgelegt, gezielt Zweifel, Misstrauen und Spaltung zu fördern. Dabei greifen sie auf verschiedene Methoden zurück, um ihre Wirkung zu maximieren. Eine der zentralen Taktiken besteht darin, Emotionen gezielt anzusprechen. Inhalte, die Angst, Wut oder Empörung auslösen, werden in sozialen Medien deutlich häufiger geteilt und verbreitet als sachliche Informationen. Durch die gezielte Emotionalisierung lassen sich Menschen leichter manipulieren, da emotionale Reaktionen häufig einer rationalen Faktenprüfung im Wege stehen.

Ein weiterer wichtiger Mechanismus ist die Nutzung algorithmischer Verstärkung. Soziale Netzwerke sind darauf programmiert, Inhalte basierend auf Interaktionsraten zu priorisieren, was dazu führt, dass polarisierende und reißerische Beiträge eine größere Reichweite erzielen. Dies begünstigt die Bildung von „Echokammern", in denen Nutzerinnen und Nutzer nur noch mit Informationen konfrontiert werden, die ihre bereits bestehenden Überzeugungen bestätigen. Dadurch verstärken sich gesellschaftliche Spaltungen und ein konstruktiver Diskurs wird erschwert.

Die gezielte Verbreitung gefälschter oder verzerrter Informationen erfolgt oft über ein Netzwerk aus gefälschten Accounts, sogenannten Bots, sowie durch den gezielten Einsatz von Influencern und Meinungsmachern, die entweder bewusst oder unbewusst Falschinformationen weiterverbreiten. Dabei kommen zunehmend auch Deepfake-Technologien zum Einsatz, mit denen manipulierte Videos und Bilder erstellt werden können, die auf den ersten Blick authentisch wirken. Diese technologischen Fortschritte machen es immer schwieriger, Wahrheit von Fiktion zu unterscheiden, und stellen eine ernsthafte Herausforderung für die Medienkompetenz der Gesellschaft dar.

Im Rahmen hybrider Bedrohungen wird Desinformation gezielt eingesetzt, um politische Gegner zu destabilisieren oder eigene Interessen durchzusetzen. Besonders autoritäre Staaten wie Russland und China nutzen strategische Desinformationskampagnen, um Einfluss auf westliche Demokratien zu nehmen und internationale Narrative zu steuern. Ein bekanntes Beispiel ist die russische Einflussnahme auf die US-Präsidentschaftswahlen 2016, bei der durch gezielte Desinformation versucht wurde, gesellschaftliche Konflikte zu verschärfen und das Vertrauen in demokratische Prozesse zu untergraben.

Ein weiteres Beispiel sind Desinformationskampagnen im Zusammenhang mit der COVID-19-Pandemie. Hier wurden bewusst Falschinformationen über Impfstoffe, die Herkunft des Virus und angebliche Verschwörungen verbreitet, um Misstrauen gegenüber Regierungen und Wissen-



schaft zu schüren. Solche Kampagnen haben das Potenzial, nicht nur politische Krisen zu verschärfen, sondern auch gesundheitliche und soziale Schäden zu verursachen, indem sie etwa die Impfbereitschaft senken oder zu Protesten gegen Schutzmaßnahmen anstacheln.

Neben der Beeinflussung von Wahlen und gesellschaftlichen Debatten spielt Desinformation auch eine Rolle in militärischen Konflikten. Im Krieg zwischen Russland und der Ukraine wurde deutlich, wie Desinformationskampagnen gezielt eingesetzt werden, um Fehlinformationen über den Kriegsverlauf zu verbreiten, westliche Unterstützung für die Ukraine zu untergraben und das Narrativ der eigenen Seite zu stärken. Die Vermischung von Desinformation mit Cyberangriffen, wirtschaftlichem Druck und militärischen Operationen macht hybride Bedrohungen besonders gefährlich, da sie schwer zu bekämpfen sind und oft erst erkannt werden, wenn der Schaden bereits eingetreten ist.

Die wirksame Bekämpfung von Desinformationskampagnen erfordert einen vielschichtigen Ansatz, der sowohl technologische als auch gesellschaftliche und politische Maßnahmen umfasst. Eine zentrale Herausforderung besteht darin, Falschinformationen frühzeitig zu identifizieren und ihre Verbreitung zu verhindern, ohne dabei die Meinungsfreiheit einzuschränken.

Ein wichtiger Ansatz ist die Förderung der Medienkompetenz in der Bevölkerung. Wenn Menschen besser darin geschult sind, Quellen kritisch zu hinterfragen, manipulative Inhalte zu erkennen und zwischen Fakten und Meinungen zu unterscheiden, sinkt die Wirksamkeit von Desinformationskampagnen. Bildungseinrichtungen, Medien und zivilgesellschaftliche Organisationen spielen eine entscheidende Rolle bei der Vermittlung dieser Kompetenzen.

Technologische Lösungen können ebenfalls dazu beitragen, Desinformation zu bekämpfen. Plattformen wie Facebook, Youtube und X stehen in der Verantwortung, gezielt gegen Falschinformationen vorzugehen, indem sie etwa irreführende Inhalte markieren, Faktenchecks durchführen und automatisierte Netzwerke zur Verbreitung von Desinformation eindämmen. Gleichzeitig birgt dies jedoch das Risiko, dass legitime Meinungen zensiert werden oder die Kriterien für die Identifikation von Desinformation politisch instrumentalisiert werden.

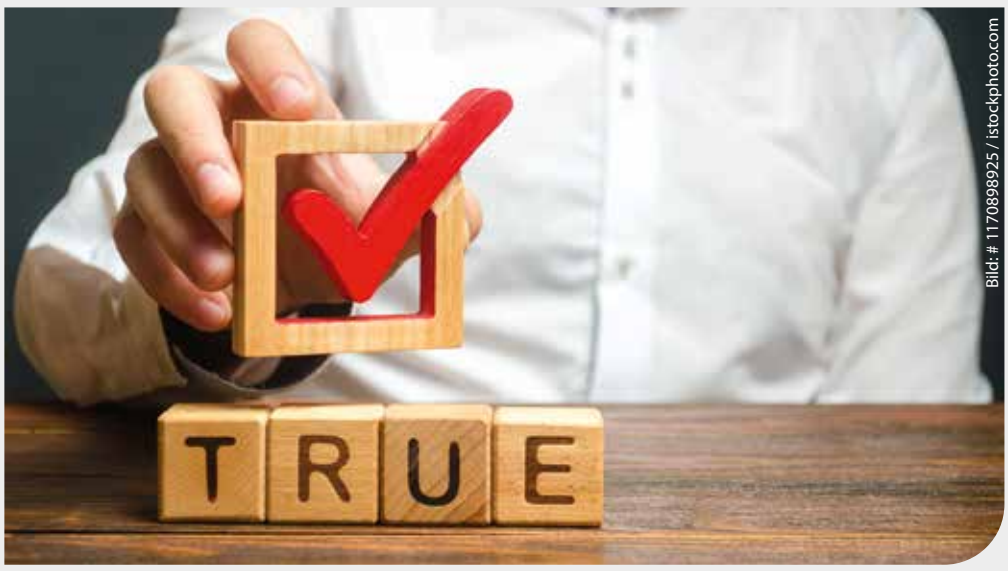


Bild: # 1170898925 / istockphoto.com

Auch staatliche Akteure müssen Maßnahmen ergreifen, um sich gegen Desinformationskampagnen zu wappnen. Dies umfasst einerseits die Stärkung der Cyberabwehr, um gezielte Angriffe auf Informationsinfrastrukturen abzuwehren, und andererseits eine transparente und proaktive Kommunikation seitens der Regierungen. Wenn offizielle Stellen schnell und glaubwürdig auf Falschinformationen reagieren, lässt sich verhindern, dass sich diese unkontrolliert verbreiten.

Internationale Zusammenarbeit ist ein weiterer Schlüssel im Kampf gegen Desinformationskampagnen. Da viele dieser Angriffe von staatlichen oder nicht staatlichen Akteuren mit globalen Interessen ausgehen, sind koordinierte Maßnahmen zwischen Demokratien erforderlich. Institutionen wie die Europäische Union oder die NATO setzen bereits verstärkt auf Strategien zur Bekämpfung von Desinformation, indem sie etwa gemeinsame Aufklärungskampagnen fördern oder Mechanismen zur schnellen Identifikation und Neutralisierung von Fake News entwickeln.

Letztlich wird der Kampf gegen Desinformationskampagnen ein fortlaufender Prozess bleiben, der sich an neue technologische Entwicklungen und gesellschaftliche Herausforderungen anpassen muss. Eine resiliente Gesellschaft zeichnet sich dadurch aus, dass sie nicht nur auf Desinformation reagiert, sondern präventiv handelt, um das Vertrauen in demokratische Prozesse, Medien und wissenschaftliche Erkenntnisse langfristig zu stärken. Nur durch eine Kombination aus Bildung, technologischer Innovation und internationaler Zusammenarbeit kann es gelingen, den Einfluss von Desinformationskampagnen als hybride Bedrohung wirksam einzudämmen.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

BSI-Lagebericht 2024

Im jährlichen Bericht gibt das BSI einen umfassenden Überblick über die Bedrohungen im Cyberraum. Laut BSI ist die Lage der IT-Sicherheit in Deutschland besorgniserregend. Cyberkriminelle professionalisieren ihre Arbeitsweisen und haben Strukturen für ihre kriminellen Dienstleistungen etabliert. Trotzdem arbeitet das BSI permanent und intensiv an einer Stärkung der Cyberresilienz.
www.bsi.bund.de

Allianz Risk Barometer 2025

Von über 3.700 weltweit befragten Risikomanagern werden Cybervorfälle, Betriebsunterbrechungen und Naturkatastrophen als die drei größten Geschäftsrisiken eingeschätzt. In Deutschland sind dies ebenfalls die drei Top-Geschäftsrisiken. Auf Platz 4 landet global und national die Änderungen von Gesetzen und Vorschriften als Geschäftsrisiko.
www.commercial.allianz.com

BfV-Flyer „Sabotage stoppen“

Seit 2023 sieht sich Deutschland mit der neuen Bedrohungsform „Sabotage durch ausländische Nachrichtendienste“ konfrontiert. Zu dieser Entwicklung tragen maßgeblich die russischen Nachrichtendienste bei. Der Flyer des BfV sensibilisiert besonders betroffene Personengruppen für entsprechende Anwerbeversuche über soziale Medien und Messengerdienste.
www.verfassungsschutz.de

UP KRITIS Empfehlungen zur Gewährleistung der Informationssicherheit

Der Zweck dieser Best-Practice-Empfehlungen ist es, die wichtigsten Sicherheitsanforderungen an die Lieferanten von Produkten/Dienstleistungen für Kritische Infrastrukturen zu identifizieren und in einer Form zur Verwendung in Vereinbarungen mit dem Lieferanten zu dokumentieren. Unter Lieferanten werden auch Dienstleister und Hersteller im Sinne einer Werkleistung verstanden.
www.bsi.bund.de

RA Dr. Berthold Stoppelkamp
zuständiges Geschäftsführungsmitglied für den Fachausschuss Wirtschaftsschutz im BDSW