Krieg ohne Grenzen? (1)

Schutz und Verteidigung gegen Gefahren aus dem Cyberraum – eine gesamtgesellschaftliche Aufgabe

Die fortschreitende Digitalisierung in allen Lebens- und Wirtschaftsbereichen liefert immer neue Angriffsflächen bei fatalerweise sinkenden Kosten und steigender Attraktivität für Angreifer aus allen Bereichen. In diesem Umfeld werden nicht mehr nur Kriminalität und Konkurrenz, sondern auch Konflikte und Kriege allerorten ausgetragen. Quasi überall in der realen und virtuellen Welt drohen Gefahren und Schäden – und daher sind auch allerorten Verteidiger gefragt: vom Staat über die Wirtschaft bis hin zum informierten Bürger. Unsere Autor:inn:en appellieren hier nicht zuletzt an die sachverständigen Cybersicherheitsprofis, diese Mammutaufgabe zu unterstützen.

Von Stefanie Frey, Siegburg, und Ramon Mörl, München

Der erste Weltkrieg wurde erst im Rückblick als der Beginn des industrialisierten Krieges – maschinelles Töten von Menschen – eingestuft. Wie wird sich der am am 24. Februar 2022 begonnene Angriffskrieg Russlands auf die Ukraine rückblickend einordnen lassen? Als „eine Zeitenwende"? Oder als der erste systematisch hybrid geführte Krieg mit Bomben, Raketen, Panzern in der realen Welt und mit Fake News, Desinformationskampagnen, Ransomware-Angriffen, digitalen Spionageaktivitäten und Cyber-Attacken in der virtuellen Welt – nicht zuletzt gegen kritische Infrastrukturen im Herzen des Industriezentrums Europa?

Die täglichen Berichterstattungen (spätestens seit der Veröffentlichung der „NTC Vulkan Files" [1]), Berichte des Bundeskriminalamts (BKA) und des BSI, aber auch von Gruppen wie Atlantic Council (bspw. „Narrative Warfare" [2]) verdeutlichen, wie all dies zu einer Gefährdung von Demokratien und ihren systemerhaltenden Wirtschaftsstrukturen beitragen kann – ausgehend von verschiedenen Akteuren mit unterschiedlichen Motiven. „Solar Winds" hat gezeigt, dass Angriffe über Lieferketten schon praktisch durchgeführt werden – „Heartbleed" und „Log4j" haben gezeigt, dass Angriffe über Elemente möglich sind, die vor langer Zeit in die Infrastruktur integriert wurden. Die „Vulkan Files" belegen eine staatliche Beteiligung an der Herstellung von Schwachstellen, die auch zur Infiltration und Kontrolle genutzt werden.

Die unlängst erfolgte Einbestellung der Geschäftsführungen von Open AI, Microsoft und Google ins Weiße Haus in Washington wegen Desinformationsgefahren durch KI-Anwendungen, die aktuell (noch) vor allem Marketing- und Internet-Branche einsetzen, unterstreichen die Gefahren hybrider Bedrohungen für alle Lebens- und Wirtschaftsbereiche.

Selbstschutz der Wirtschaft

Ohne demokratische gesellschaftliche Stabilität ist auch keine nachhaltige Stabilität für Unternehmen in den demokratischen Wirtschaftsnationen möglich. Schutz und Verteidigung gegen systemgefährdende Informationen im Cyberraum lassen sich in Autokratien und Einparteiensystemen wie China leichter und einfacher organisieren als in Demokratien mit starker Freiheits- und Beteiligungs-Orientierung. Umso mehr sind hier alle Akteure gefragt – auch außerhalb staatlicher Strukturen.

Fake News sind eben nicht nur für die Gesellschaft oder die Politik eine Gefahr, sondern gerade auch für (systemerhaltende) Unternehmen und kritische Infrastrukturen: Kaufentscheidungen, die ja auf Basis von freier Information getroffen werden, können durch Fake News manipuliert werden. Wenn sich eine Fake News festsetzt, dass etwa ein bestimmtes Produkt eines Unternehmens schlechter, unsicherer oder instabiler ist als ein vergleichbares Produkt, obwohl dies objektiv falsch ist, können schnell Wettbewerbsnachteile entstehen. Nicht umsonst dürfen in der Werbung keine Lügen verbreitet werden und es erfolgt eine entsprechende Strafverfolgung und Durchsetzung – was sich im Fall von schlechter attribuierbaren Fake News und Cyberattacken jedoch aktuell schwierig gestaltet.

Deshalb ist es höchste Zeit für alle: Bürger, Cybersicherheits-Fachleute und -Entscheider in Unternehmen sowie Verwaltungen und Politik in demokratischen Wirtschaftsnationen müssen die komplexen Zusammenhänge von Digitalisierung, Auswirkungen auf freie Wissens- und Meinungsbildung und Cyber-Sicherheit verstehen. Die Grenzenlosigkeit im Cyberraum erfordert es, Angriffsvektoren aus unterschiedlichen Sphären und neue Formen von Manipulationen der Meinungsbildung auch in Unternehmen und Organisationen zu berücksichtigen.

Aus diesem Verstehen heraus lassen sich wirksame und robuste Schutz- und Verteidigungs-Maßnahmen ableiten – selbst kurz- und mittelfristig. Nur so werden in demokratischen Gesellschaften, in Deutschland, in der EU und international, alle resilienter. Nur so werden wir die liebgewonnenen und nicht mehr wegzudenkenden Werkzeuge unserer Zeit (Computer, Internet, Smartphones, ...) weiterhin guten Gewissens im privaten, wirtschaftlichen und öffentlichen Leben weiter nutzen können – Werkzeuge, die mittlerweile auch für die weitere Wertschöpfung in der Wirtschaft und damit für die Wohlstandserhaltung unerlässlich geworden sind.

Der vorliegende Beitrag ist der erste einer dreiteiligen Serie und behandelt zunächst Fake News als Wegbereiter und Begleiter hybrider Bedrohungen und Kriegsführung. In den nächsten Ausgaben der <kes> werden Teil 2 zu „Cyber in War“ und Teil 3 zu Schutz und Verteidigung der Bürger sowie der ansässigen Industrie gegen Gefahren aus dem Cyberraum folgen.

Fake News

Laut BITKOM geben drei Viertel der Internetnutzer in Deutschland an, dass ihnen die Verbreitung von Falschinformationen in den sozialen Medien Sorgen macht [3] – besonders zum Ukraine-Krieg. Auch nach Erkenntnissen der Initiative D21 e. V. erachten 64 % der Bevölkerung Desinformationen als eines der größten Risiken der Digitalisierung für die Demokratie [4]. In einer Eurobarometer-Umfrage sahen sogar 83 % der Teilnehmer:innen in Fake News eine zunehmende Bedrohung für unsere Demokratien [5].

„Cyberangriffe können unter Umständen gefährlicher sein für die Stabilität von Staaten und Unternehmen als Panzer und Gewehre ...“, äußerte der ehemalige EU-Kommissionspräsident Jean-Claude Juncker schon Mitte September 2017 in seiner Rede zur Lage der Europäischen Union [6]. Und die „High Level Expert Group“ (HLEG), eine hochrangige interdisziplinäre 39-köpfige unabhängige Gruppe, eingesetzt durch die EU-Kommission, hat Fake News und Online-Desinformation im März 2018 eine 44-seitige Bestandsanalyse nebst Handlungssträngen mit Zeitplan zum Umgang mit systemgefährdenden Desinformationen gewidmet [7]. Die Liste ließe sich beliebig fortsetzen.

„Lügen scheint zum Handwerk nicht nur der Demagogen, sondern auch des Politikers und sogar des Staatsmannes zu gehören“, hat Hannah Arendt 1963 in ihrem klassischen Essay „Wahrheit und Politik“ geschrieben. Damals gab es keinen Aufschrei. Warum auch? Konrad Adenauer selbst pflegte mit ironischem Lächeln zwischen der einfachen, der reinen und der lauteren Wahrheit zu unterscheiden [8].

Wo in den 1960ern jedoch viel Aufwand und Geld nötig waren, um Propaganda zu verbreiten – so viel Geld, dass selbst KGB und CIA (im Vergleich zu heute) wenig erfolgreich waren –, ist im Internetzeitalter mit „Cybercrime as a Service“ (CaaS), Bots und Hilfsmitteln wie ChatGPT so etwas für wenige hundert Euro zu haben. Und mithilfe von Social-Media-Plattformen gibt es genügend sogenannter Echo-Kammern (siehe Kasten auf S. 18), um Lügen, Propaganda und Manipulationen tausendfach, ja millionenfach verstärkt in die Welt zu bringen.

Image-Missbrauch und -Schäden

Angriffe auf Organisations-/Unternehmens-IT haben „klassischerweise“ vorrangig kommerzielle Ziele, also etwa Geld zu erpressen oder Wettbewerbsvorteile durch das Ausspähen von Information zu erzielen. Immer bedrohlicher werden aber auch fehlerhafte Darstellungen von vermeintlichen Firmeninformationen im Internet und die Manipulation durch Deep Fakes – je nach gesellschaftlicher oder politischer Lage. Das BSI warnt beispielsweise vor dem sogenannten Spoofing, also etwa der Nutzung vorgeblicher BSI-Telefonnummern zur Verbreitung von Desinformation und der Vorbereitung von Cyberattacken.

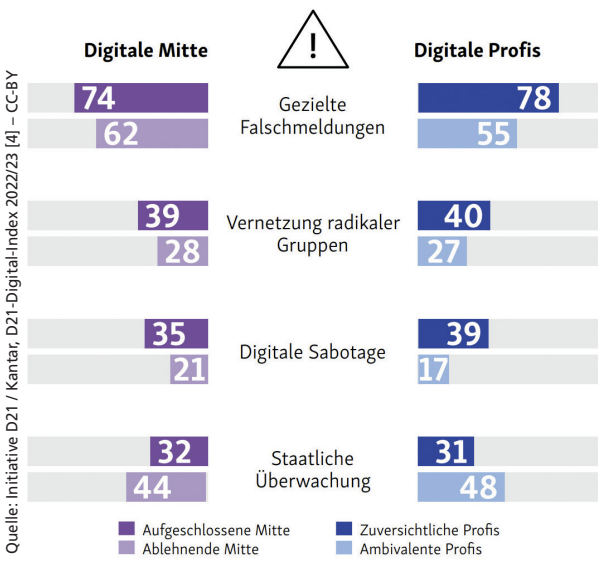


Abbildung 1: Risiken der Digitalisierung laut D21-Digital-Index 2022/23 [4]

Basis: Bevölkerung ab 14 Jahren (n = 6.087), Angaben in Prozent „unter den Top-3-Risiken“

Gleichermaßen leidet das Image von Banken und Sparkassen unter erfolgreichen Angriffen mit ihren Logos und Kundenkontakten. Und angefangen mit professionell über Bots infiltrierten Verunglimpfungen von Unternehmen und ihren Produkten bis hin zu unwahren Beschreibungen schlechter Arbeitsbedingungen und ähnlichen „weichen" Zielen, kann eine einmal „erfundene" Information und Technologie leicht in die Hände der falschen Internet-Teilnehmer fallen – oder beispielsweise die Datenbasis für Kaufentscheidungen verfälschen, ohne dass benachteiligte Unternehmen überhaupt Kenntnis davon hätten.

Open-Source-Intelligence-(OSINT)-Analysen nutzen heute künstliche Intelligenz (KI), um globale Trends, Stimmungen und Stichworterwähnungen zu identifizieren. Dabei werden die in öffentlichen Quellen wie Fernsehen und Rundfunk, Social Media und Websites verfügbaren Daten analysiert, um verwertbare Erkenntnisse zu liefern und gegebenenfalls Falschinformation zu Unternehmen aufzuspüren. Das nachhaltige Löschen solcher Falschinformationen ist für Unternehmen eine große Herausforderung, denn zum einen sind nicht alle Informationsbereiche in der digitalen Welt einsehbar und zum anderen benötigt die gesetzliche Durchsetzung des Löschens auf ausländischen Servern langwierige Verfahren, während derer die Informationen immer noch im Umlauf sind und schädlich bleiben.

Seit vielen Jahren werden zunehmend Angriffe auf Demokratien beziehungsweise die Werte der Demokratie verzeichnet. Ziele sind dabei allem voran die Destabilisierung der demokratischen Staaten und – damit eng verbunden – eine steigende Handlungsunfähigkeit in diesen Staaten. Nur einige wenige Beispiele sind die Berichterstattungen von Influencern wie Alina Lipp mit rund 180 000 Followern, die dem russischen staatlichen Narrativ nahestehen und behaupten, dass die Ukraine „entnazifiziert" werde [9], oder Meldungen des immer noch aktiven – wenn auch in der Zwischenzeit in Deutschland verbotenen Senders – RT Television oder Falschmeldungen wie im „Fall Lisa" [10] während der Flüchtlingskrise 2015/2016, bei dem nach dem eintägigen Verschwinden eines deutsch-russischen Mädchen nicht zuletzt in russischen Staatsmedien verschiedene Entführungs- und Vergewaltigungsgeschichten „hochgekocht" waren, die sich später als unzutreffend herausstellten. Derartige „Informationsattacken" sind etwa geeignet, die Polizei – und damit die Exekutive – zu diskreditieren, Ausländerfeindlichkeit zu schüren und sogar diplomatische Spannungen heraufzubeschwören.

Forschung und Aufklärungsarbeiten

Eine Studie [11] des gemeinnützigen „Center für Monitoring, Analyse und Strategie" (CeMAS) bringt es auf den Punkt: „Desinformation darf nicht nur als Informations- oder Sicherheitsproblem verstanden werden. Es ist ein Angriff auf die Demokratie als solches." Das Gleiche gilt auch für die Werte der von Desinformation betroffenen Unternehmen oder Wirtschaftszweige.

Mehrere vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekte beschäftigten sich detaillierter mit dem Thema der Desinformation und Fake News. So trugen unter anderem Prof. Dr.-Ing. Dorothea Kolossa von der Technischen Universität Berlin und Prof. Dr. Martin Emmer von der Freien Universität Berlin Mitte März 2023 auf der „Nationalen Konferenz IT-Sicherheitsforschung 2023 – Die digital vernetzte Gesellschaft stärken" zum Thema Fake News und Gefährdung demokratischer Werte vor. Auch wenn Konferenz-Teilnehmer vor Ort dem Staat jegliche Fähigkeiten zum zeitnahen Erkennen von Fake News abgesprochen haben, wurde die Kernproblematik dennoch deutlich [12].

Bereits bei der „Digitalen Berliner Sicherheitskonferenz – Stabilität Mitteleuropas (BSC) 2021" bestand nach Einschätzung vieler Teilnehmer kein Erkenntnisproblem, sondern ein signifikantes Handlungsproblem [13].

Weitere unscharfe Punkte bedürfen noch einer Konkretisierung, beispielsweise: Was genau ist eine demokratiegefährdende und damit mittelbar auch Wirtschaftssystem-gefährdende (Des-)Informations-/Fake-News-Kampagne? Wer hat eventuell ein Recht zur Beeinflussung von Meinungen in demokratischen Prozessen? Ab wann ist eine staatliche Gegenmaßnahme Zensur und/oder Markteingriff?

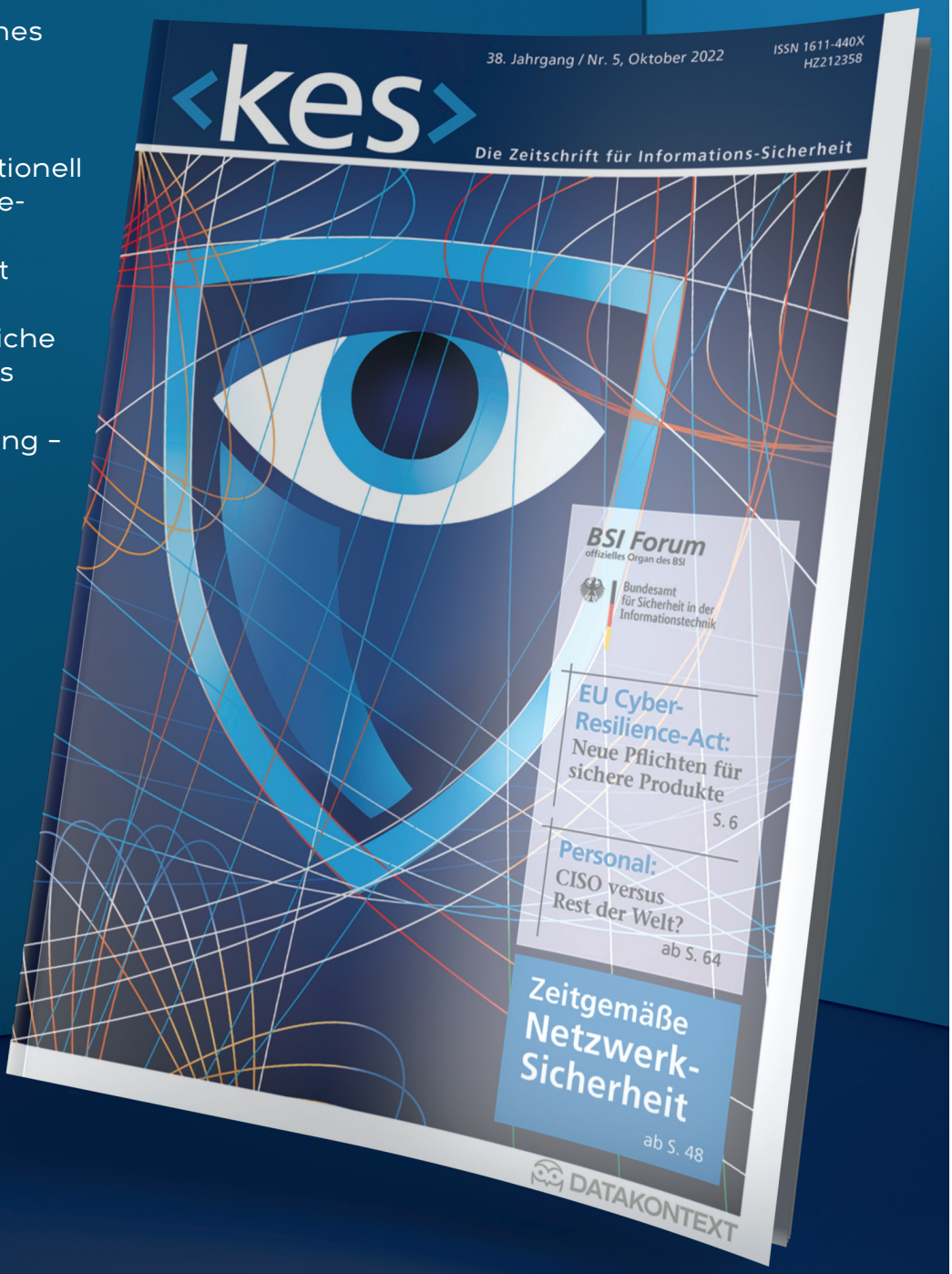
Unabhängig davon handelt es sich beispielsweise bei der Beeinflussung von Wahlen durch Drittstaaten eindeutig um eine Gefährdung der Demokratie – und mittelbar auch um eine Beeinflussung von etwaigen nachteiligen Sicherheits- und Wirtschaftsregulierungen. Solches Handeln bedarf sofortiger Gegenmaßnahmen!

Insofern ist das möglichst zeitgleiche Weiterverbreiten von Fakten und transparent nachvollziehbaren Positionen in den betroffenen Echokammern eine der wichtigsten Aufgaben bei der Bekämpfung der Effekte systemgefährdender Fake News für Unternehmen und Organisationen in Demokratien.

Der Frage, ob die einschlägigen Echokammern und Webseiten hauptsächlich durch Menschen hergestellt oder bereits voll automatisiert durch Algorithmen und Bots generiert werden, (und vielen anderen Fragen rund um das Thema) geht ein Papier der Universität Düsseldorf von 2019 nach, das auf einer internationalen Konferenz in Hawaii vorgestellt wurde [14].

Need to know für CISO & Co.

- <kes> liefert strategisches Wissen für Security-Verantwortliche
- <kes> informiert redaktionell unabhängig zu Management und Technik der Informations-Sicherheit
- <kes> enthält das amtliche Organ des Bundesamts für Sicherheit in der Informationsverarbeitung – BSI-Forum
- <kes> kostet im Jahr weniger als zwei Beraterstunden



<kes>
Die Zeitschrift für Informations-Sicherheit

Für 159,00 € jährlich (inkl. MwSt. und Versandkosten) erhalten Sie alle zwei Monate eine gedruckte Ausgabe und für bis zu fünf Mitarbeiter am belieferten Standort Online-Zugriff auf alle aktuellen Beiträge sowie das <kes>-Archiv.

Online bestellen: datakontext.com/kes
oder per Mail: abo@kes.de

DATAKONTEXT

Sprache formt und begrenzt Denken und Handeln

Eine korrekte Diskussion um Schutz und Verteidigung sowohl der Werte der Demokratie als auch der systemerhaltenden Unternehmen (bes. in Schlüsselindustrien) und Organisationen im sich durch neue Technologie schnell verändernden Internet benötigt eine klare Begriffsbildung, denn unsere Sprache formt und begrenzt gleichzeitig unser Denken und Handeln.

_____ Was ist ein Cyberangriff, was sind die Instrumente eines Cyberangriffs?
_____ Wann lassen sich auch Fake News als Angriff werten?
_____ Wann ist eine Verteidigung „aktiv"?
_____ Wann werden demokratische Werte und Prozesse der Willensbildung, systemerhaltende Grundwerte oder wesentliche Informationen zu Unternehmen im Cyberraum angegriffen?
_____ Ab welchen Schwellwerten müssen Schutz und Verteidigung stattfinden?
_____ Wie können sich Unternehmen und Organisationen effektiv und schnell wehren, wo doch das Internet nichts vergisst und schlechte Nachrichten, egal wie unwahr sie sein mögen, weite Verbreitung finden?
_____ Wie kann/darf sich ein Unternehmen gegen Fake News wehren?

Die Antworten auf solche Fragen und die verwendbaren Begriffe müssen standardisiert werden, um überhaupt eine gesamtgesellschaftliche und vor allem internationale Diskussion – auch innerhalb der NATO – führen zu können. Auf Basis solcher Begriffsdefinitionen wäre es dann möglich, Prozesse der Schutz- und Verteidigungs-Maßnahmen von Unternehmen und Organisationen zu standardisieren, wie diese etwa beim Eindringen unidentifizierter Flugkörper in den nationalen Luftraum nach „9/11" definiert wurden und von NATO-Verbündeten mit zugesicherten Zeiten von deutlich unter 10 Minuten bis zum physischen Eingreifen geübt werden.

Beispiel: Definition von Cyber-Angriff/-Angreifer

Was ist eigentlich ein Cyber-Angriff und wer ist der Angreifer? Intuitiv scheint das völlig klar zu sein: Ein Nicht-Berechtigter – der Angreifer – will einem Schaden zufügen und nutzt dafür IKT-Mittel. Doch so einfach lässt sich dem Thema leider nicht begegnen. Man betrachte hierzu etwa das Beispiel eines Produkts aus einem Drittland: Eine Firma hat ein Internet-of-Things-(IoT)-Gerät gebaut, einen über WiFi vernetzen Rauchmelder, der in Smart-Buildings eingesetzt wird. In manchen Ländern oder auf Firmengeländen soll in dem Produkt eine Kamera und ein Mikro verbaut sein, damit die Feuerwehr sich im Brandfall sofort einen Überblick verschaffen kann, wo

Echokammern/Bubbles erfordern kurze Reaktionszeit

Im Internet, den sozialen Medien oder auch dem Darknet bilden sich – wie in der „analogen" Welt (z. B. durch Pegida) – Gruppen Gleichdenkender. Diese Gruppierungen schaffen dann häufig ihre eigenen Kommunikationsgruppen, die als Echokammern oder als Social-Media-Blasen (Bubbles) bezeichnet werden. Kurz gefasst handelt es sich um sich selbst bestärkende und verstärkende Informationsverteilungsmechanismen. In der Präsidentschaftswahl in den USA, aus der Donald Trump als Sieger hervorging, wurde ein Management solcher Bubbles im Wahlkampf genutzt, um Wähler zu gewinnen.

So kann man jeweils innerhalb einer Bubble relativ einfach Zustimmung erlangen, da durch deren Mitglieder kein Vergleich mit Informationen erfolgt, die man in anderen Communitys streut, weil sie an diesen anderen Communitys nicht teilhaben. Die über alle Communitys hinweg gestreuten Informationen können dadurch beliebig widersprüchlich sein – und man „trifft" die Wünsche und Meinungen vieler.

Aus den Beobachtungen in verschiedenen sozialen Medien zu problematischen Fake News hat sich folgende Erkenntnis herausgebildet: Nach der initialen Adressierung einer Falschmeldung in einer „Echo Chamber" oder einer „Bubble" bleiben nur circa 2 Stunden zur Schadensminimierung, um dieser Falschmeldung eine wahre Darstellung entgegenzusetzen. Der Hintergrund liegt darin, dass man einerseits dem „Kern" dieser Gruppe ohnehin kein anderes Narrativ (erfolgversprechend) anbieten kann. Andererseits bringen durch die schnelle digitale Verbreitung neu hinzukommende Personen innerhalb dieser Zeitspanne noch Aufmerksamkeit für das Thema auf und denken – falls geeignete Informationen in geeigneter, also für dieses Medium üblicher Darstellung vorliegen – auch über den Wahrheitsgehalt der verschiedenen Darstellungen nach, sodass sie gegebenenfalls die Weiterverbreitung der Falschmeldung nicht noch selbst unterstützen.

Heutzutage ist jeder Nutzer im Internet Informationskonsument, aber gleichzeitig auch Informationsgeber, indem er/sie Informationen multipliziert oder (weiter-) verteilt. Die Vertrauensstellung des Senders und die Häufigkeit der in kurzer Zeit von vielen „Quellen" eintreffenden ähnlichen Information wird beim Empfänger unterschwellig zur Beurteilung des „Wahrheitsgehalts" von Information herangezogen.

Flammen sind, wo noch Personen eingeschlossen sind – und falls überall Rauch ist, soll man über das Mikro eventuelle Schreie hören.

Damit das Produkt schneller auf den Markt kommt, ist ein erfahrener Freiberufler beauftragt worden, einen Treiber für den Kommunikations-Stack in das IoT-Produkt einzubauen. Der Programmierer implementiert diesen und liefert in Zeit und Qualität ab – der Auftrag bezieht sich dabei lediglich auf die umzusetzende Funktionalität, nicht aber auf die Sicherheit von eventuellen Angriffen. Der Freiberufler hat, um komplexe Tests einfacher durchführen zu können, eine offene Schnittstelle eingebaut und dokumentiert, wie diese vor dem Verkauf des Produkts deaktiviert werden kann beziehungswesie soll. Bei der Zusammenstellung des Produkts wird diese Deaktivierung jedoch vergessen – somit bleibt das IoT-Device (neben evtl. anderen Schwachstellen) auch über diese Schnittstelle angreifbar.

Im Produkt gibt es Softwareschalter (Konfigurationen), mit denen sich Kamera und Mikro aktivieren und deaktivieren lassen, um es so für unterschiedliche Märkte und deren Datenschutzvorstellungen anzupassen. Das erschien im Rahmen der Produktplanung kosteneffizienter und leichter, als für die verschiedenen Märkte unterschiedliche Geräte zu entwickeln und auszuliefern.

Ein Mitarbeiter der Herstellerfirma weiß um den mit einem Standardpasswort geschützten Testzugang, wird gekündigt, ist unzufrieden mit seiner Kündigung und verkauft sein Wissen über das Internet an ihm unbekannte Dritte. Diese setzen diese Erkenntnisse auf ihre Zero-Day-Liste, bauen einen Exploit und verkaufen alles zusammen als Service – inklusive Nutzung des Exploit-Kits mit Anleitung und Funktions-Garantie. Im Exploit-Kit gibt es die Varianten „Kamera und Mikro anschalten und gefundene Daten ausleiten“ sowie das Infiltrieren von Angriffsvektoren, die das betroffene Netzwerk auskundschaften, um Angriffe auf andere Komponenten und Infrastruktur zu fahren – etwa um in die Voice-Over-IP-(VoIP)-Kommunikation einzubrechen.

Dieser Cyber-Angriff folgt einer ganzen Kette von Ursächlichkeiten: „Vergessen“, „Rache wegen schlechter Behandlung“, „Softwareschalter statt Hardwareschalter“ (ein Hardware-Kippschalter bspw. gäbe dem Eigentümer die Kontrolle über Kamera/Mikrofon) et cetera.

Selbst die Haftung ist diesem Beispiel nicht eindeutig zuzuordnen: Haftbar wäre eventuell auch jemand, der den Rauchmelder eingebaut hat, von der Problematik aber gar keine Kenntnis hatte und sich „nur“ nicht vorher überzeugt hat, dass keine Hintertür in dem Produkt enthalten ist (falls das überhaupt möglich erscheint). Viele weitere Fragen bleiben unklar:

_____ Wer hat den Angriff verursacht?
_____ Wer ist schuldig?
_____ Wer kann haftbar gemacht werden nach welchem Recht?
_____ Welche Regulierung oder welches Recht wurden überhaupt verletzt?
_____ Was könnte man in der Folge einklagen (bspw. das Löschen der privaten Videoaufnahmen über den Rauchmelder)?

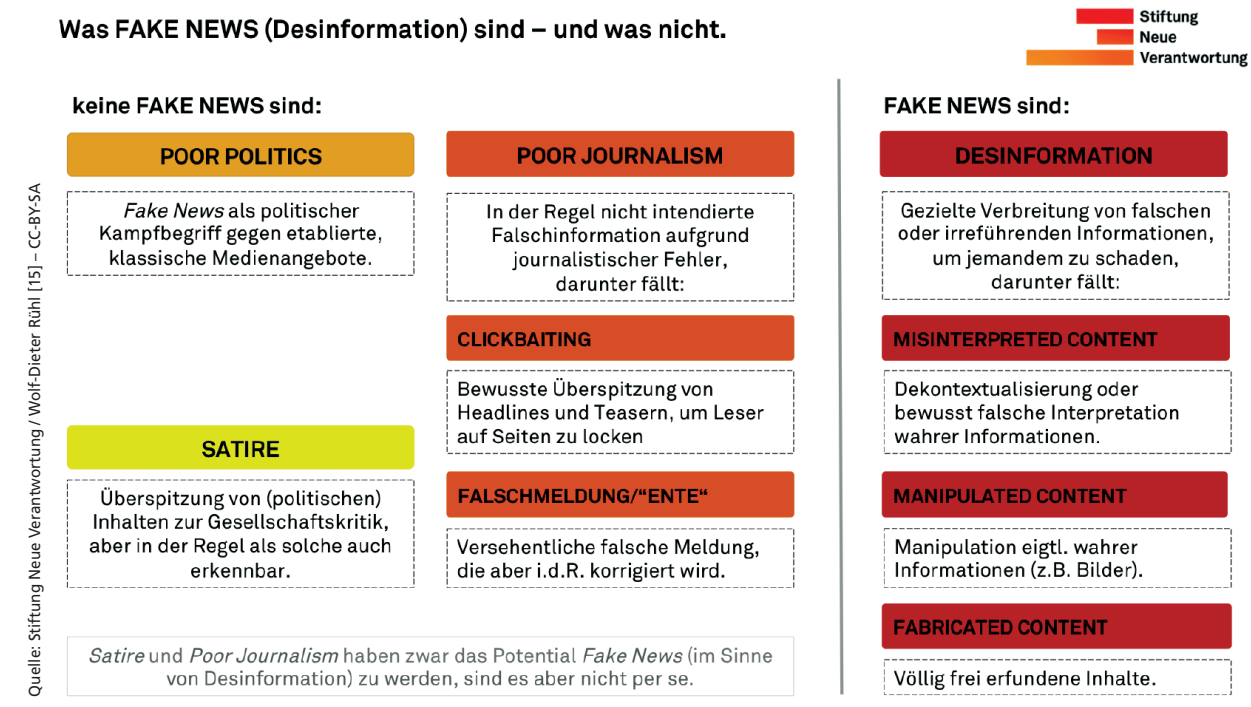


Abbildung 2: Abgrenzung von Fake News zu anderen falschen oder irreführenden Informationen

Annäherung an eine Fake-News-Definition

Auch für Fake News gibt es noch keine standardisierte Nomenklatur. Abbildung 2 zeigt eine mögliche Einordnung der Stiftung Neue Verantwortung (SNV) [15].

Nicht jede Fake News ist zudem geeignet, Unternehmen, Organisationen, demokratische Entscheidungen oder Grundwerte anzugreifen. Nicht jede Fake News kann von jedem sofort als solche entlarvt werden.

Häufig setzen Fake News auf einem wahren Kern auf und bilden dann um diesen herum eine Falschmeldung: Ist es zum Beispiel in dem bereits erwähnten „Fall Lisa" valide, der Polizei, deren Reputation unter der Fake News leidet, die Verteidigung ihrer Reputation zu überlassen? Wer wäre dann dafür zuständig, wenn im deutschen Cyberraum etwa verbreitet wird, dass Russland eine Entnazifizierung der Ukraine durchführt? Es ist sogar bereits unklar, was genau „der deutsche Cyberraum" oder der „unternehmenseigene Cyberraum" überhaupt sein soll.

Was ist also zu tun? Das Thema, das keine eindeutig beweisbare Lösung haben kann, endlos diskutieren und dadurch jede Handlung verhindern? oder anhand von klaren Beispielen wie dem Angriff auf den Bundestag, der sicherlich nationaler Cyberraum ist, Prozesse und Zuständigkeiten erarbeiten und diese in klaren Fällen kurz- und mittelfristig anwenden, um damit beispielhafte Handlungsmodelle für Unternehmen aufzuzeigen?

Zensur

Zensur beschreibt Prof. Dr. Oliver Bendel, FHNW, Hochschule für Wirtschaft, Institut für Wirtschaftsinformatik, wie folgt „Über Zensur werden unerwünschte oder unerlaubte Inhalte verhindert, beschnitten oder verfälscht. Sie kann sowohl Text als auch Bild betreffen" [16].

Es geht also nicht darum, dass zusätzliche Information, zum Beispiel Gegendarstellungen, als Zensur gesehen werden. Vielmehr ist es gerade ein demokratischer Grundwert, dass die freie Meinungsäußerung es ermöglicht, auf Defizite oder Falschmeldungen in einer Darstellung hinzuweisen. Zensur wird meist staatlichen Stellen unterstellt und ist als solche sehr negativ bewertet. Gute, zeitnahe Darstellungen anderer Fakten zu Fake News werden deshalb von manchen Teilen der Bevölkerung staatlichen Stellen grundsätzlich nicht zugetraut. Wie eine potenzielle Kooperation aussehen kann, welche die nationalen Fähigkeiten und die Vertrauensketten in der Bevölkerung zusammenführt, ist eine offene Frage.

Freiheitswerte versus Zensur

In Deutschland ist die Angst vor Zensur und Markteingriffen sicher auch historisch bedingt hoch. Vor allem scheint es so zu sein, dass die Bürger die Bewertung des Wahrheitsgehalts von Information ungern in den Händen des Staates sehen, wenn es um „freie" Information im Internet geht. Ein Präsident einer Bundesbehörde stellte in seiner Rede die These auf: Wenn ein Auto mit Kameras auf dem Dach durch die Straßen fährt und es steht Google darauf, dann winken viele Leute – wenn BND darauf stünde, gäbe es großen Ärger.

Wenn wir also als Gesellschaft den Kampf gegen eine Verfälschung der Datenbasis für Entscheidungen bis hin zur Erosion der demokratischen Werte durch Fake News aufnehmen und uns für eine klare unverfälschte Unternehmenskommunikation einsetzen wollen, sind folgende Faktoren zu berücksichtigen:

_____ Es gibt keine saubere Trennschärfe, welche Falschmeldungen Unternehmen, Organisationen oder die Demokratie als solche gefährden.

_____ Es gibt keine stabilen Vertrauensketten zwischen Gesellschaft, Unternehmen und Staat und zwischen Staaten untereinander.

_____ Es gibt nur einen sehr kurzen Reaktionszeitraum (unter 2 Std.), um Fake News transparent ermittelte Fakten und begründete nachvollziehbare Wahrheiten in der gleichen Echokammer entgegenzustellen und damit relativierend und meinungsbildend wirken zu können.

_____ Man muss die Sprache der betreffenden Echokammern verwenden (Wortwahl, Bildsprache etc.), um überhaupt meinungsbildend wirken zu können.

_____ Der Zugang zur Echokammer, in der die Fake News ihre Wirkung entfaltet, ist für staatliche Stellen oft mit restriktiven Auflagen versehen und für Unternehmen allein wegen der Menge der Echokammern schier unmöglich.

Fazit

Fake News – gerade in staatlich oder professionell und automatisiert eingesteuerter Form – lassen unsere Demokratie und die Werte der Demokratie erodieren, gefährden Unternehmen wie Bürger und sind Wegbereiter für systemgefährdende Cyberangriffe. Sie verfälschen die Datenbasis zur Meinungsbildung und damit wichtige Entscheidungen – ob privat, in Unternehmen oder anderen Organisationen. Das Ziel der Akteure ist, die Handlungsfähigkeit der westlichen demokratischen Staaten zu verringern, Unternehmen zu diskreditieren oder aus dem Markt zu drängen. Durch Volksbewegungen, die instrumentali-

siert werden, oder anderweitige Abwanderung der Wähler aus der Mitte der demokratischen Gesellschaft, gelingt es zunehmend, die Demokratie und ihre systemerhaltenden Unternehmen und Organisationen zu destabilisieren.

Die Dienste, die OSINT-Beobachter der nationalen Stellen, haben beste Erkenntnisse – sie handeln aber nicht. Alle Beteiligten sind sich einig: Es liegt kein Erkenntnisproblem, sondern ein Umsetzungsproblem vor. Der Beitrag des Satirikers Jan Böhmermann „Die Polizei ist nicht im Internet“ (https://youtu.be/WQXmj0nOQHw) hat beispielsweise Defizite in der Strafverfolgung aufgezeigt. Manche Bürger verlieren das Vertrauen in den Staat, glauben gegebenenfalls nicht länger, dass er ihre Interessen geeignet wahrnimmt. Andere sehen im Internet die letzte Bastion, wo sie ihren Gedanken der Informationsfreiheit freien Lauf lassen können.

Lösungsansätze könnten beispielsweise umfassen, Erkenntnisse öffentlicher Stellen (Behörden, Dienste) und eventuell privater Quellen (anonymisiert) zertifizierten Akteuren wie NGOs (bspw. NAFO, https://nafo-ofan.org), vertrauenswürdigen Bürgern im Ehrenamt oder bei besonders kritischen Themen auch Unternehmen, die unter Geheimschutzbetreuung stehen, zur Verfügung zu stellen. Diese Akteure und Fakten-Checker könnten auf die ermittelten Informationen zugreifen und gleichzeitig fundierte Klarstellungen geliefert bekommen, sodass sie zeitnah in die mit Fake News belasteten Informationsräume eintreten und die gemeinsamen Werte der Demokratie verteidigen könnten.

Wesentlich für den Erfolg wäre bei diesem Ansatz die mediale Steuerung, in welcher der Staat seine grundsätzlichen Handlungsschwierigkeiten in der Verteidigung gegen Fake News darstellt, die in eng gesetzten Rechtsrahmen liegen, die, um das Vertrauen der Bürger zu erhalten, nicht aufgebrochen werden dürfen.

Der Staat gibt in der physischen Welt Steuergelder für die Sicherheit der Bürger aus: nächtliche Beleuchtung, damit Kinder auch spät im Winter sicher auf der Straße sind, Geschwindigkeitsbegrenzungen bei Schulen, um bekannte Risiken zu minimieren, Verbot elektrischer Produkte, die Sicherheitsnormen nicht erfüllen, et cetera. Im Cyberraum existiert jedoch bisher kein vergleichbarer wirksamer praktischer Schutz als Infrastruktur für Bürger und ansässige Unternehmen und Organisationen.

Öffentliche Stellen bieten stattdessen in der Regel eher Empfehlungen und komplexe Handreichungen an, wie Bürger und Unternehmen sich schlau machen und sich sowie die eigene Infrastruktur selbst absichern können oder sollen. Ob der chinesische Staubsaugerroboter aus dem örtlichen Elektronikmarkt, der aus welchen Gründen auch immer permanente Netzverbindung verlangt, die Gespräche und Wohnsituation unter Umständen „nach Hause“ meldet oder nicht, sollen die Bürger selbst prüfen – oder die Stiftung Warentest. In der Umsetzung des Onlinezugangsgesetzes (OZG, www.onlinezugangsgesetz.de) kommt die pragmatische und praktische Cybersicherheit bislang ebenfalls deutlich zu kurz.

Der Schutz und die Verteidigung der Bürger sowie der ansässigen Unternehmen ist zu einem gewissen Teil aber auch Aufgabe des Staates, die er am besten in Kooperation mit vertrauenswürdigen Know-how-Trägern übernimmt, um Schlüsselkompetenzen nicht weiter zu verlieren. Digitalisierung ist nicht optional und braucht Vertrauen in die digitale Welt! Solches Vertrauen lässt sich aufbauen, wenn Steuergelder außer zur Sensibilisierung für Fake News, Desinformation und Angriffsvektoren auch direkt und effektiv spürbar in geeignete IT-Security bei Schutz- und Infrastrukturmaßnahmen sowie in die Stärkung der praktischen Abwehr von Fake News und Desinformation fließen. Ein gutes Beispiel ist etwa der Aufbau des European Digital Media Observatory (EDMO, https://

Chat-GPT, Bots und Troll-Farmen

ChatGPT ist ein Chatbot, der künstliche Intelligenz (KI) einsetzt, um mit Nutzern über textbasierte Nachrichten zu kommunizieren. Er nutzt moderne maschinelle Lerntechnologie, um Antworten zu generieren, die natürlich klingen und für das Gespräch relevant sein sollen. Die Problematik besteht darin, dass es damit nunmehr Software gibt, die in relativ korrekter Sprache vorgegebene Inhalte umsetzt und auch auf Kommentare zu diesen Themen mit Antworten reagieren kann, die einem definierten Ziel folgen – und das in vielen Sprachen.

Bereits früh wurde bekannt, dass verschiedene Länder sogenannte Troll-Farmen aufgebaut haben: Diese sollte man sich ähnlich wie Callcenter als eine größere Ansammlung von Mitarbeitern vorstellen, die an einem vorgegebenen Ziel arbeiten. Je nach intellektueller Ausbildung der Mitarbeiter können sie nur bereitgestellte Textbausteine in Echokammern einbringen oder auch Chats zu diesen Themen sinnvoll weiterführen.

Durch die Verbesserung der Algorithmen, die zunehmend solche Aufgaben übernehmen, ist die Skalierung nahezu unbegrenzt und das Antrainieren neuer Inhalte und Ziele sehr einfach geworden. Wie so oft in der digitalen Welt und bei Fake News ist also nicht das Thema neu, wohl aber die Skalierung: Die Möglichkeiten, in kurzer Zeit unglaublich große Mengen an gezielten Desinformationen zu streuen und die Aufrechterhaltung der Desinformation in Chats gegen andere zu verteidigen, ist durch ChatGPT enorm gewachsen.

edmo.eu) und seiner nationalen oder multinationalen Hubs (Knotenpunkten) wie das German-Austrian Digital Media Observatory (GADMO, https://gadmo.eu) – ein Netzwerk, das darauf abzielt, Desinformation zu bekämpfen und ihre Auswirkungen auf Gesellschaft und Demokratie sowohl auf nationaler als auch auf europäischer Ebene zu analysieren und operativ richtig zu stellen. ■

Dr. Stefanie Frey ist Geschäftsführerin der Deutor Cyber Security Solutions. Ramon Mörl ist Geschäftsführer von itWatch.

Literatur

[1] Christoph Cadenbach, Ben Heubl, Lena Kampf, Georg Mascolo, Mauritius Much, Max Muth, Natalie Sablowski, Lea Weinmann, Ralf Wiegand, Vulkan Files – Im Netz der Krieger, Exklusive Einblicke in die Waffenkammer von Putins Cyberarmee, Süddeutsche Zeitung, März 2023, www.sueddeutsche.de/projekte/artikel/politik/cyberkrieg-russland-propaganda-desinformation-cyberattacke-wladimir-putin-recherche-leak-ukraine-ukrainekrieg-hacking-e585517 (kostenpflichtig)

[2] Nika Aleksejeva, Andy Carvin, Narrative Warfare, How the Kremlin and Russian outlets justified a war of aggression against Ukraine, Atlantic Council / DFRLab, Februar 2023, www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/

[3] Dr. Bernhard Rohleder, Wie die Deutschen auf den Ukraine-Krieg reagieren, Vortragsfolien, März 2022, www.bitkom.org/sites/main/files/2022-03/Bitkom-Charts%20Verbraucherumfrage%20Ukraine%2022%2003%2022.pdf

[4] Initiative D21 e. V., D21-Digital-Index 2022/23, Jährliches Lagebild zur Digitalen Gesellschaft, Februar 2023, https://initiatived21.de/app/uploads/2023/02/d21_digital_index_2022_2023.pdf

[5] European Union, Fake news and disinformation online, Eurobarometer Publication Report, März 2018, https://europa.eu/eurobarometer/surveys/detail/2183

[6] Europäische Kommission, Präsident Jean-Claude Juncker, Rede zur Lage der Union 2017, September 2017, https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_17_3165

[7] European Commission Directorate-General for Communication Networks, Content and Technology, A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, März 2018, https://coinform.eu/wp-content/uploads/2019/02/EU-High-Level-Group-on-Disinformation-A-multi-dimensionalapproachtodisinformation.pdf

[8] Rolf Steininger, Der Alte im Fegefeuer, Frankfurter Allgemeine Zeitung, Nr. 217, September 2004, S. 9, www.faz.net/aktuell/feuilleton/politik/der-alte-im-fegefeuer-1179929.html

[9] ZDFheute, Russische Propaganda trotz EU-Verbots, November 2022, www.zdf.de/nachrichten/zdfheute-live/propaganda-russland-deutschland-influencer-video-100.html (Video verfügbar bis 2023-11-17)

[10] Wikipedia, Fall Lisa, https://de.wikipedia.org/wiki/Fall_Lisa

[11] Pia Lamberty, Lea Frühwirth, Ein Jahr russischer Angriffskrieg, Die Rolle von Desinformation in Deutschland, Center für Monitoring, Analyse und Strategie (CeMAS), Februar 2023, https://cemas.io/publikationen/desinformation-und-angriffskrieg/

[12] Prof. Dr. Martin Emmer, Prof. Dr.-Ing. Dorothea Kolossa, Prof. Dr. Nicole Krämer, Prof. Dr.-Ing. Christian Grimme, David Schraven (Moderation), Mit Forschung Fake News bekämpfen, Session 3.2 der Nationalen Konferenz IT-Sicherheitsforschung 2023, März 2023, www.forschung-it-sicherheit-kommunikationssysteme.de/nationale-konferenz-it-sicherheitsforschung-2023/programm/sessions

[13] Digitaler Staat online, Digitale Berliner Sicherheitskonferenz – Stabilität Mitteleuropas, Mai 2021, www.digitaler-staat.online/2021/05/13/digitale-berliner-sicherheitskonferenz-2021-stabilitaet-mitteleuropas-2/

[14] Franziska Zimmer, Katrin Scheibe, Prof. Wolfgang G. Stock, Mechtild Stock, Echo Chambers and Filter Bubbles of Fake News in Social Media: Man-Made or Produced by Algorithms?, in: 2019 Arts, Humanities, Social Sciences & Education Proceedings, Januar 2019, https://huichawaii.org/ahsse/proceedings-programs/proceedings-ahse-2019-2-2/

[15] Wolf-Dieter Rühl, Measuring Fake News – Die Methode, Stiftung Neue Verantwortung, Dezember 2017, www.stiftung-nv.de/sites/default/files/fake_news_methodenpapier_deutsch.pdf

[16] Oliver Bendel, 350 Keywords Digitalisierung, Springer Gabler, April 2019, ISBN 978-3-658-25823-8, https://doi.org/10.1007/978-3-658-25823-8 (kostenpflichtig)